Universidade de Aveiro
2008
Departamento de Electrónica, Telecomunicações e Informática

André Gonçalo Gabriel de Campos

Estudo de Mecanismo de Mobilidade Intra e Interdomínio


Universidade de Aveiro
2008
Departamento de Electrónica, Telecomunicações e Informática

André Gonçalo Gabriel de Campos

Estudo de Mecanismo de Mobilidade Intra e Interdomínio

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica do Prof. Dr. Rui Aguiar, Professor auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

Dedico este trabalho aos meus pais e irmãos por todo o apoio que sempre me deram e que possibilitou a minha chegada até aqui.

o júri

presidente

Doutor José Luís Guimarães Oliveira
Professor Associado da Universidade de Aveiro

vogais

Doutor Manuel Alberto Pereira Ricardo
Professor Associado do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade De Engenharia da Universidade do Porto

Doutor Rui Luís Andrade Aguiar (Orientador)
Professor Associado da Universidade de Aveiro

agradecimentos

Ao Professor Rui Aguiar por tudo o que me ensinou não só a nível de docência mas como exemplo de como saber encarar a vida a nível profissional e por ter acreditado em mim.
À Professora Susana Sargento que desde o meu primeiro dia nesta academia até ao último me apoiou e me soube ajudar a balançar a calma com a energia em trabalho.
Aos meus colegas e amigos do HNG (Heterogeneous Networking Group), e em especial ao Vitor Jesus, por toda a ajuda e por me mostrarem que o trabalho pode ser feito com alegria.
Aos meus amigos por todos estes bons anos que me proporcionaram.
À minha namorada, Francisca, por toda a paciência e apoio que deu durante a elaboração desta tese.
E por último, a mais importante, à minha família, simplesmente porque tudo lhes devo.

palavras-chave

Mobilidade IP, Handover, dominio administrativo, federação, intra-dominio, inter-dominio.

resumo

Desde a invenção da roda e dos sinais de fumo que o Homem tem como umas das suas grandes preocupações o poder mover-se e comunicar. Esta tese vai discutir o que se passa quando o homem quer comunicar em movimento, e falar sobre mobilidade associada ao protocolo IP nas suas duas divisões: intra-domínio e inter-domínio focando-se especialmente numa nova proposta para um protocolo de mobilidade, o ESM.

ESM, também conhecido por *Eppur si muove* é uma proposta que pretende ser uma solução completa e eficiente para a mobilidade IP. Abrange mobilidade intra-domino e inter-domínio e é uma arquitectura inteiramente operada pela parte da rede, tem um serviço central de localização em cada domínio o que permite saber onde estão os nós moveis e usa endereçamento não hierárquico que possibilita que possam existir endereços IP com o prefixo diferente do utilizado em determinada localização. Foi por isto tudo que foi escolhido como principal objecto de estudo neste trabalho.

Esta tese irá concentrar-se na arquitectura ESM com as suas diferentes opções e novos melhoramentos, incluindo resultados da sua simulação em NS-2 para testar o comportamento do ESM e provar que é um mecanismo rápido e eficiente como se pretende. Irá também apresentar alguns outros protocolos que suportem mobilidade, tal como MIP, CIP, HAWAII, SIP entre outros.

keywords

IP Mobility, Handover, administrative domain, federation, intra-domain, inter-domain.

abstract

Since the invention of the wheel and smoke signals that Men has at high concerns the ability to move and communicate. This thesis will discuss what happens when Men want to communicate while is moving and talk about mobility associated with IP protocol in its two divisions, intra-domain and inter-domain with a special focus on one new proposal to a mobility protocol, ESM. ESM, also known as, *Eppur si muove* it's a proposal that intends to be a complete and efficient solution to mobility using IP. It covers the intra-domain and the inter-domain mobility and it is an architecture entirely operated by the network side, has one central service of location on each domain that allows to know where are the mobile nodes and uses a flat IP that allow to have IP address with prefixes different of the IPs on that location. Was because all this that was chosen as the principal study of this work

This thesis will focus on ESM architecture with the different options and new improvement solutions including its simulation and results using NS-2, to test ESM behavior and to prove that it can be a fast and efficient mechanism as it claims to be. It also presents some other mobility protocols like MIP, CIP, HAWAII or SIP among others.

Contents

List of Figures

List of Tables

Acronyms

Acronym	Description
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AAAF	Authentication, Authorization and Accounting server in Foreign Domain
AAAH	Authentication, Authorization and Accounting server in Home Domain
AP	Access Point
AR	Access Router
BA	Binding Acknowledgement
BR	Border Router
BS	Base-station
BU	Binding Update
CBR	Constant Bit Rate
CIP	Cellular Internet Protocol
CN	Correspondent Node
CoA	Care-of Address
CoR	Cross over Router
DAIDALOS	Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimized personal Services
DHCP	Dynamic Host Configuration Protocol
DSDV	Destination Sequenced Distance Vector
EN	Edge Node
ESM	Eppur si muove
FA	Foreign Agent
FBACK	Fast Binding Acknowledgement
FBU	Fast Binding Update
FMIP	Fast Mobile Internet Protocol
	Continue on next page

Acronym	Description
FTP	File Transfer Protocol
FwR	Forwarding Router
GFA	Gateway Foreign Agent
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GW	Gateway
HA	Home Agent
HACK	Handover Acknowledge
HAR	Home Anchor Router
HAWAII	Handoff-Aware Wireless Access Internet Infrastructure
HD	Home Domain
HI	Handover Initiate
HMIP	Hierarchical Mobile Internet Protocol
HNG	Heterogeneous Networking Group
HO	Handover
HSDPA	High-Speed Downlink Packet Access
H-SIP	Handle Session Initiation Protocol
HSUPA	High-Speed Uplink Packet Access
IETF	Internet Engineering Task Force
IMS	Internet Protocol Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
L3-FHR	Layer3-Frequent Handoff Region
LA	Location Acknowledgement
	Continue on next page

Acronym	Description
LCoA	Local Care-of Address
LMD	Localized Mobility Domain
LS	Location Service
LU	Location Update
MAP	Mobility Anchor Point
MIFA	Mobile Internet Protocol Fast Authentication
MIP	Mobile Internet Protocol
MIPv4	Mobile Internet Protocol version 4
MIPv6	Mobile Internet Protocol version 6
MN	Mobile Node
MWIF	Mobile Wireless Internet Forum
nAP or NAP	New Access Point
nAR or NAR	New Access Router
NCoA	New Care-of Address
NDP	Neighbor Discovery Protocol
NetLMM	Network-based Localized Mobility Management
NOAH	No Ad-hoc Routing Protocol
NS-2	Network Simulator 2
oAR	Old Access Router (same as Previous Access Router)
PA	Precedence Address
pAP or PAP	Previous Access Point
pAR or PAR	Previous Access Router
PCoA	Previous Care-of Address
PMIP	Proxy Mobile Internet Protocol
QoS	Quality of Service
RCoA	Regional Care-of Address
SIP	Session Initiation Protocol

Continue on next page

Acronym	Description
SLA	Service Level Agreement
TA	Transit Address
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifiers
VAR	Visited Access Router
VD	Visited Domain
VOIP	Voice Over Internet Protocol

Chapter 1

Introduction

There are currently needs of communication everywhere. We want to make a phone call, send a SMS, receive an email, consult news on the Internet or do something else and we want to do it no matter where we are, if we are stopped, walking, in a freeway or jumping around. We just need, want, desire to communicate.

Advances in technology are growing faster in order to satisfy our wishes, but the truth is that we want more and more and more: GSM (Global System for Mobile communications, 1991), GPRS (General Packet Radio Service, 1997), UMTS (Universal Mobile Telecommunications System 2000), HSDPA (High-Speed Downlink Packet Access) and HSUPA (High-Speed Uplink Packet Access), (May, 2007) give us an idea about the pressing evolution in mobile networks, trying to answer this society hunger.

It is widely accepted that networks are converging to IP based protocols. We can see it in VOIP (Voice Over Internet Protocol) that it's a set of protocols that allow an optimization in the transmission of the voice over the Internet. VOIP starts to substitute in some homes or companies the traditional phone. Other emergent service is the IPTV (Internet Protocol Television) that is already in many of our homes and provides features like Video on Demand in opposite to the old single analogical television.

There is a lot of research work done (and other that remain to be done) in mobility in IP networks, trying to find solutions for these mobile communicating needs. Mobility brings some challenges to network topologies. What previously were stable and organized topologies using wired nodes only, could now be a confusion with wireless nodes, if they decide to move to different positions of the original. The hierarchical topology concept that allows small routing tables don't work because the prefix of the IP address of a mobile node may not correspond to the prefix of the Access Router that

currently serves it, if new solutions like Mobile IP didn't appear. But Mobile IP is one (maybe the most promising), but not the unique solution to solve this and other problems when Handover issues appear.

A handover, or handoff, is different from the common roaming. In roaming, one network allows a mobile node from other network to connect in it and use its service. It implies a previous agreement between the operators and the user receives a bill from the original operator with both charges. In a handover, the act of moving from one place to another is maintained as is roaming, but this moves possible the transferring of ongoing flow of traffic (a call or simple data) without closing a connection and restart again. A handover could be done between two access routers of the same administrative domains (and is designed as an intra-domain handover) or between two distinct domains (and is called an inter-domain handover).

The biggest problem in inter-domain mobility has to do with how end-to-end sessions control is split by two administrative domains. It is needed a previous agreement between domains, that decides the permissions, rights and degree of information exchanged, as well as the terms of technical interoperation when the domain interact with others.

Several proposals of mobility protocols try to solve all these mobility problems, but that is not an easy task. This some extensions appeared to solve only small problems of other proposals, like route optimization with Fast Mobile IP and Hierarchical Mobile IP trying to solve triangular route or delays in signaling. Other proposals go for different approaches and divide mobility in local and global mobility. Some works discuss only local mobility, with some improvement in handover executions and packets delivery, like Cellular-IP or HAWAII, or avoiding the involvement of the terminal in the Handover execution, as in NetLMM.

The mobility proposed designed inside HNG (Heterogeneous Networking Group), ESM (*Eppur si muove*), is a protocol that aims to be:

i) efficient;

ii) without the need of intervention by the terminal, which means that is entirely operated by the network part;

iii) complete, since it could be deployed as an intra-domain and inter-domain architecture.

The work done in this thesis was the refinement of the ESM architecture, with the main goal to test it using Network Simulator 2. From simulations, we extracted some results in times of registration, delays and loss of packets that prove that ESM architecture is as it claimed to be: fast and efficient in intra and inter-domain mobility.

The reminder of the thesis is divided in 4 more chapters. In Chapter 2 it's discuss what is IP mobility and some current solutions of intra-domain and inter-domain mobility, while Chapter 3 is dedicated to ESM. Chapter 4 is where the simulation results are presented and Chapter 5 draw final conclusions and discusses future work.

Chapter 2

IP mobility

2.1 - Definition

The IP mobility concept appears with the need of moving inside a network that uses the IP protocol. In an IP network each node has its IP address according to its position on the topology of the network. So it could turn on in one position, connect to the network, then turn off and turn on in other position again, but it couldn't move between different points and maintain its connection, since it needs to break it.

With the growing mobility needs of our world and with the ideal that all networks will be eventually transformed on IP network, the idea of IP mobility is growing in importance and the research for solutions to allow the free moving in an IP network starts to increase.

The first problem with mobility is to move the terminal physically. With antennas, wireless emitters, wireless receptors, coding, decoding, etc this could be achieved. But it is also needed to find a way for an IP network to work with terminals outside its logical positions, without rewriting all the definitions of the existent and widely implemented network based on IP protocols.

With this problem statement, several proposals to protocols that allow IP mobility appeared. The most well-known will be presented in the next sections.

2.2 – Intra-domain and inter-domain

There are two main types of IP mobility: intra-domain and inter-domain.

As the name indicates the intra-domain mobility occurs inside an administrative domain and could imply mobile nodes, access routers, core routers and servers of that domain. No matter what the elements that compose the domain and participate in the handover or the signaling messages are exchanged, they all are administrated by the same entity. That means that it uses the architecture adopted by that administration, the whole domain follows consistent definitions and protocols, having the correct rights and permissions to exchange information and technically prepared for a coherent operation.

In the case of inter-domain mobility it implies the involvement of, at least two different administrative domains and not less than one node that makes a handover between them. There exists an interoperation between elements from the two domains participating in a handover, like MN (Mobile Node), pAR (previous Access Router) and pAP (previous Access Point) from the home domain and a nAR (new Access Router) with a nAP (new Access Point) from other foreign domain. All these elements need a coordination that allows the handover to be done, which could be provided by other elements of the networks.

This necessary coordination needs a previous agreement between domains, which define how the handover will be executed, its signaling exchange and the new way that the delivery of packets will occur. This is what an inter-domain mobility protocol defines.

It's also needed to agree in which degree the domains will interoperate, and what privileges they have when interacting with a different administrative domain, as how much information they exchange. That is defined in the federation agreement they have to each other. For instance there are various types of federation classes in DAIDALOS [19] (an EU Framework Programme Integrated Project in network architectures that investigate new generation communication infrastructures): from the lowest, that is considered the inexistence of federations, to the highest where the two domains act like they are only one, passing through gradual increase of permissions and information exchanged.

2.3 – Mobile IP

Mobile IP is the most significative IP mobility protocol.

2.3.1 – Classic Mobile IP

Mobile IP (MIP) [1][6] is an extension to the Internet Protocol (IP) proposed by the Internet Engineering Task Force (IETF) to support intra and inter-domain mobility between users with portable devices, without changing its IP address.

In its home network, the mobile node has an IP address corresponding to this initial location. When a packet enters the network, it is the address in the destination field of its packet header that helps to decide the next-hop (until reaching the final destination). This decision is prefix based routing on higher bits of the address because they represent the network where the destination is. If the host moves to another network, its original IP address is not usefully anymore because the routing isn't set for this new network, so the host won't ever receive packets there. To solve this, the IETF proposed that each mobile node should have two IP addresses with a transparent binding between them: the Home Address, that is a permanent address; and a Care-of-Address (CoA), that is a temporary address corresponding to a new address on the new network where this node is connected. There are also two kinds of agents:

Home Agent (HA) – Usually a router in the home network that maintains a table with the Home Address and the corresponding Care-of-Address. This table is in form <permanent home address, temporary care-of address, association lifetime>;

Foreign Agent (FA) – Usually a router in the foreign network that maintains a table with the foreign nodes in that network, making the correspondence between the Home Address and the HA address. This table has the information about <permanent home address, home agent address, media address of the mobile node, association lifetime>.

MIP works in four stages: Agent Discovery, Registration, In Service and Deregistration.

1) In the Agent Discovery stage, mobility agents send periodically broadcast messages, named Agent Advertisement, that inform the mobile node about the presence of a HA or a FA. It's possible that a mobile node sends an Agent Solicitation to request an advertisement of the Agents, if it does not want to wait for the periodic advertisement.

2) In the Registration stage, as show in Figure 2.1, the mobile node (MN) detects its current location and if it is in a new network, it sends a Registration Request containing its home address and HA address to the FA. When this is received, the Foreign Agent sends to the HA a new Registration Request, in name of the MN, with the information of the MN's care-of-address and its own address. By its turn, the HA update the mobility binding with the association between the home address of MN and its CoA, and sends an acknowledge message back to the FA, that will update its visitor list with MN information and reply to MN too.

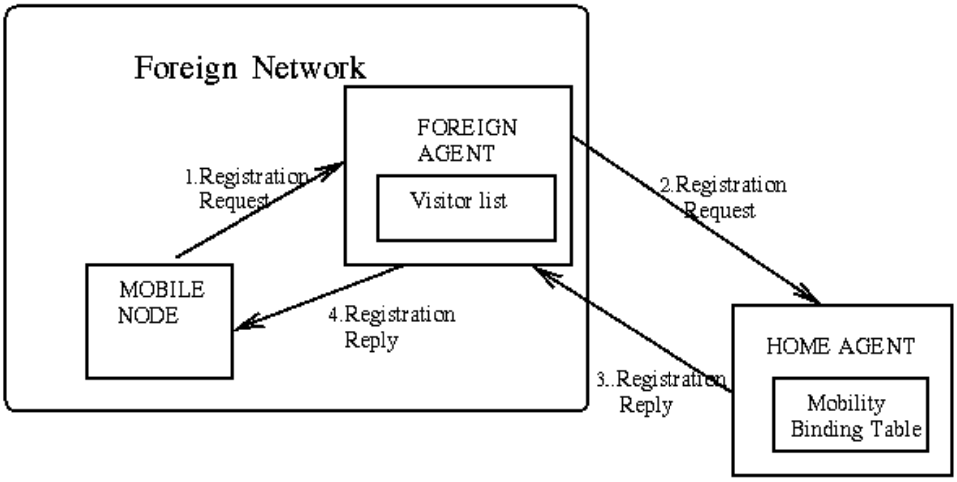

Figure 2.1: MIP registration [1]

Figure 2.2 summarizes this signaling during registration.

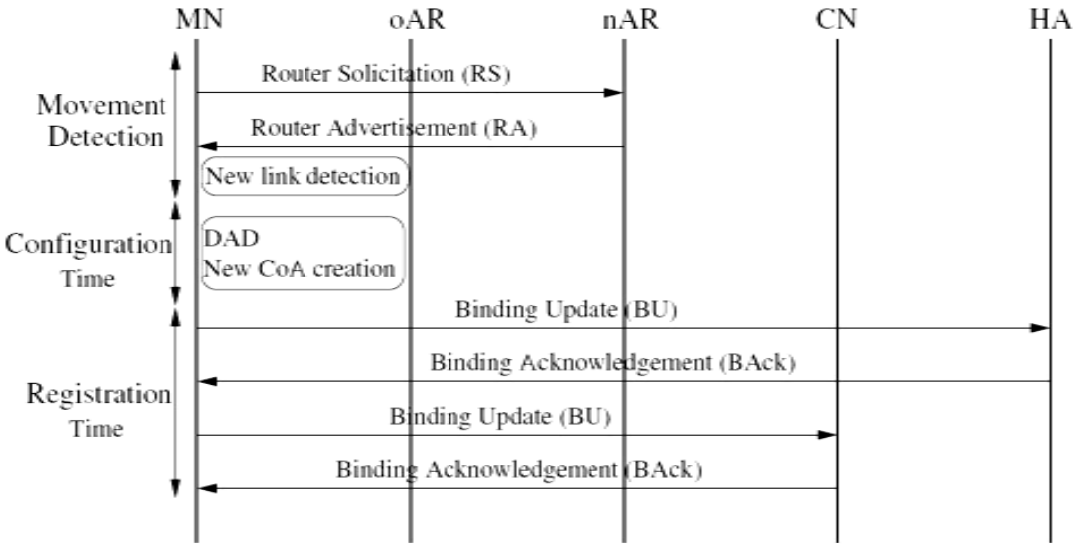

Figure 2.2: MIP registration signaling [4]

3) The In Service stage describes the way packets will reach the MN in a foreign network. When a correspondent node (CN) sends a packet to the MN, it puts in the destination field of the IP header the permanent home address of mobile node. This packet is intercepted by the HA that checks the mobility binding table and finds where the MN is located. If it is on another network, the HA takes the correspondent CoA address and makes a new IP header with it to encapsulate the IP packet into the payload (IP-within-IP encapsulation). Then this encapsulated packet reaches the FA, that decapsulates it to know the home address IP, checks the visitors list and sends it to correspondent MN. In the reverse traffic, from MN to CN, mobile node sends packet to FA that forwards it in the normal way to its destination. This route difference makes a triangle as show in Figure 2.3.

4) Deregistration is the stage were the mobile node drops the CoA because was moved to a new network. To do this, the MN needs to send a Registration Request to HA with the lifetime field set to zero. In the FA,

when the lifetime becomes zero, it automatically expires the registration, so there isn't any need to receive any kind of advertisement.

MIPv6 [6] is Mobile IP for IPv6, instead of for IPv4, the version described above. The IPv6 solves some problems of the common MIPv4. The Route Optimization [1], that is one extension in MIPv4, allowing CN sending packets directly to CoA, and solving the triangular route using binding caches, is intrinsically part of MIPv6. It has also new features like Neighbor Discovery and Address Autoconfiguration, which makes obsolete the usage of external Foreign Agents.

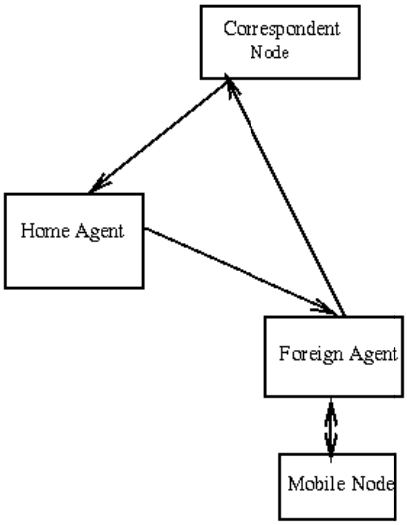

Figure 2.3: Triangular route [1]

In Mobile IPv4, when a mobile node communicates with a correspondent node, it puts its home address as the source address of the packet. Thus "ingress filtering routers", used to filter out the packets by its source address, is different from the network from which the packet originated. This problem is tackled in Mobile IPv6 by putting the care-of address as the source address and having a Home Address Destination field, allowing the use of the care-of address to be transparent over the IP layer.

This way, MIP can make mobility transparent to the higher level protocols without making larges changes to the existing network infrastructure.

2.3.2 – Fast MIP

The need to perform a registration on the HA, often far away, the handover process in MIP usually slow.

To reduce the delay in communication caused by handover in Mobile IP there are some proposed solutions. Between them is FMIP (Fast Mobile IP) [2][3][5][6] that is an extension of MIPv6.

This protocol allows to the MN to anticipate an L2 handoff based on L2 triggers. These triggers have information about link layer connection of MN and other entities.

When the mobile node discovers a new Access Point (nAP) by receiving an L2 trigger, it sends a Router Solicitation for Proxy (RtSolPr) to the previous Access Router (pAR), with the identifier of the nAR where nAP is attached. The pAR replies with a Proxy Router Advertisement (PrRtAdv) informing about the recommended new CoA, the IP and link layer addresses of the new AR and sends also to the nAR, a Handover Initiate message (HI) which contains the old CoA and the proposed new CoA of MN.

Then the nAR sends a Handover Acknowledge message (HACK) to pAR with the address of nCoA considering it as valid address. So pAR sends the fast binding acknowledgement (FBACK) message to MN and to the nAR, and establishes an IP tunnel between pCoA (previous CoA) and nCoA (new CoA) that will be in use until the MN completes the binding updates with its CNs.

When MN receives the PrRtAdv confirming the pending L3 handover, it sends a Fast Binding Update (FBU) to pCoA, before breaking the connection between them, informing it to start forward all packets to the nCoA via nAR. The pAR also sends a Fast Binding Acknowledgement (FBACK) to MN and to nAR with the final nCoA.

Now the MN is able to make the layer 2 handover, breaking the link with pAR and connecting to nAR. After arrival on the nAR it sends a Fast Neighbor Advertisement (FNA) destined to nAR, requesting that it forwards packets destined to the nCoA of the MN and if all is ok, the nAR replies to MN with a Fast Neighbor Advertisement Acknowledgment

(FNAack). Figure 2.4 illustrates the FMIP registration signaling between MN, nAR and oAR (old Access Router) that is another designation to pAR.

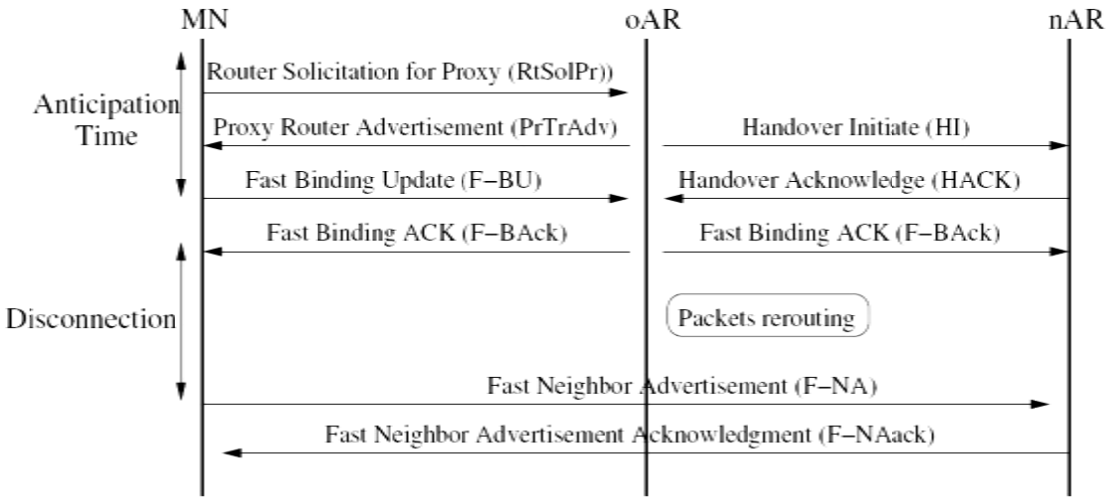

Figure 2.4: FMIP registration [4]

2.4 – Intra-domain mobility

Multiples protocols for intra-domain mobility have been proposed. We will address a couple here: HMIP, CIP, HAWAII and NetLMM.

2.4.1 - Hierarchical MIP

Hierarchical Mobile IPv6 [6][7][8] (HMIPv6) was created in order to reduce the signaling traffic of BU in MIPv6 when MN's moving away from their domain.

MIPv6 handles local and global mobility in the same way and the amount of signaling between CNs and the HA causes long registration delays and packet loss. HMIPv6 differentiates local mobility from global, being a localized mobility management

proposal. The mobility management inside a domain is handled by a Mobility Anchor Point (MAP), which basically acts as a local Home Agent, and between MAP domains is handled by MIPv6. The MAP domains are not administrative domains, but domains inside an administrative domain.

When a mobile node enters in a new MAP domain, it registers with it and obtains a Regional Care-of Address (RCoA) and a Local Care-of Address (LCoA). Then it will use the RCoA to register with HA and CNs, informing its current location and the LCoA will be used in local mobility. The MAP uses a binding cache to store mapping between RCoA and LCoA and intercepts packets that arrive to its domains with MN as destiny, encapsulating and forwarding them to the correspondent LCoA. The binding cache is maintained with periodic binding updates from MN to MAP that still continues to send BU to HA as in MIP. The registration signaling details are illustrated in figure 2.5.

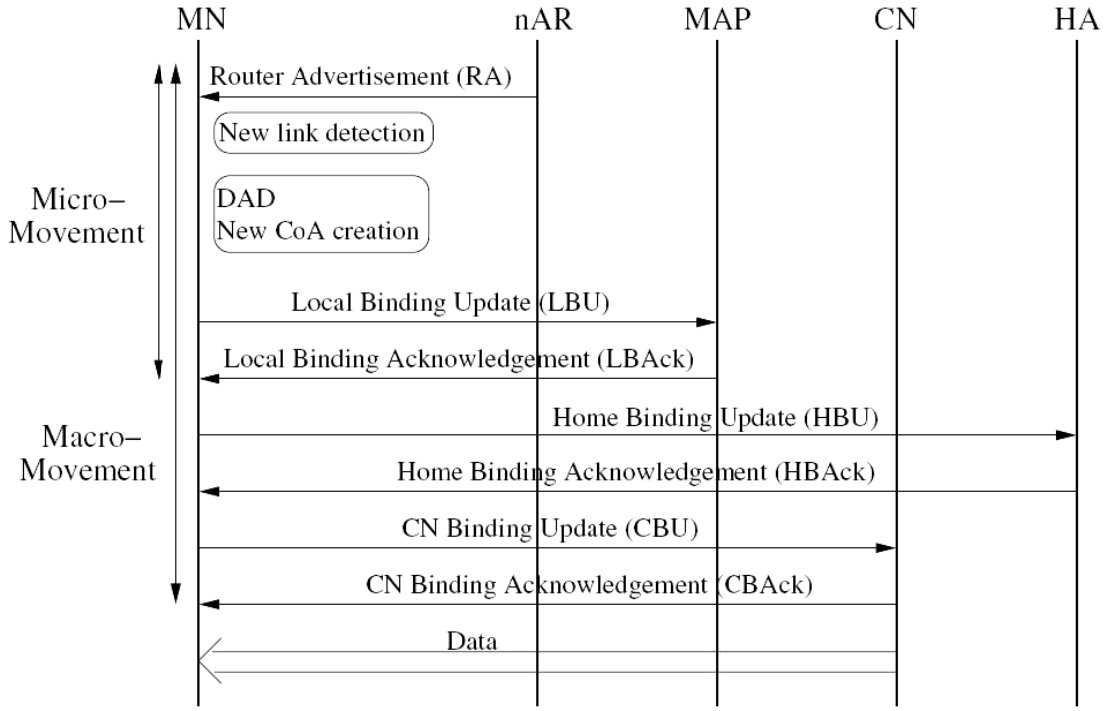

Figure 2.5: HMIP registration [4]

If a MN moves within the current MAP domain, it only needs to inform the MAP and receives a new LCoA and the local CNs, maintaining the same RCoA avoiding the need of update the HA.

The HMIPv6 advantages in reducing the signaling load only works depending on the mobility of MNs and if the handovers are inside a MAP domain because if they aren't, MIP will need to handle them.

2.4.2 – Cellular IP

Cellular IP [9][10][11] (CIP) was created essentially to complement Mobile IP and designed to optimize mobility inside a domain. So when in use, this protocol coexists with MIP. CIP will care only with mobility inside a CIP domain, and leave MIP to handle mobility between CIP domains.

A CIP domain, represented in figure 2.6, contains several nodes and access points all using CIP routing instead of the MIP routing, which means that the mobile node needs to have CIP installed too. There is also one CIP gateway (GW), in the top of the domain, which is responsible for connecting with other domains.

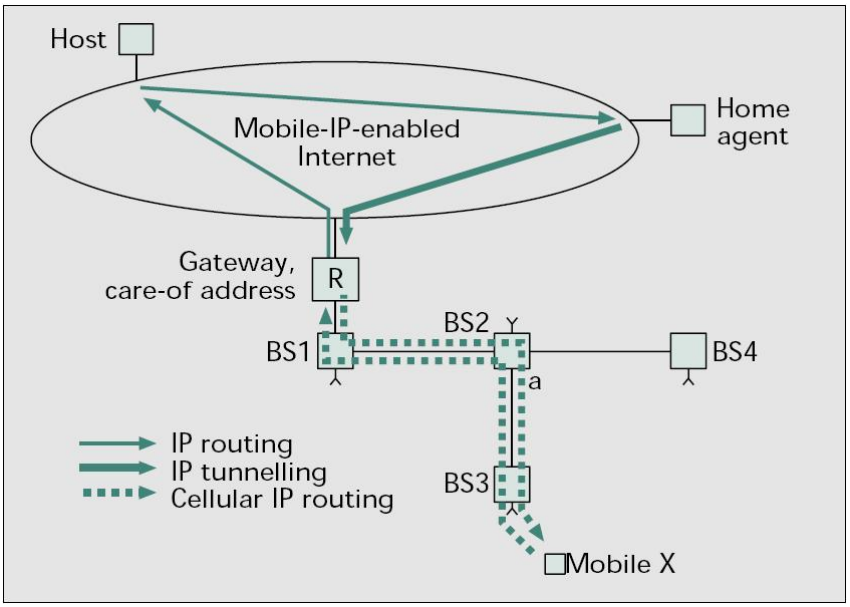

Figure 2.6: CIP access network [11]

In CIP routing there are no tunnels like in MIP and all terminals have a roll of entries with direct routes from the AP to the GW, but each one only indicates the next hop. So a packet sent by the MN is directed hop by hop to the GW. Each router extracts the IP address of the MN from the packets and saves it with the interface identifier by which the packets arrived, to a segment in database. It is the concatenation of those segments that makes the bi-directional route between MN and GW. Mobile nodes need to send at least one packet every three seconds and if they fail three consecutive packets it causes a route timeout that eliminates that particular register from the database.

The handover of MN to a new AP can be done in two ways:

A) If the mobile node can only "listen" one AP at a time, it makes a so called "hard handover". Through the use of specify CIP beacons, the terminal detects that it isn't in the same position and that there is another AP nearer, with a stronger signal. Then it sends a route update message to the new AP that forwards it to GW. In each router that it passes, the database registers the interface that delivers the packet to it, making the new route to MN. When reaching the common point between the old and new route (crossover node) this route detects that the serving AP has changed and redirects the flow of traffic to the new one, as show in figure 2.7.

B) If the mobile node has the ability to "listen" two APs at the same time, it occurs a semisoft handover. When the signal level falls below the disconnection threshold and the MN detects a stronger signal from another AP, it sends a Semisoft message to that new AP and returns to the old AP frequency. That Semisoft packet will build the new route and after a Semisoft delay the MN performs a regular handover.

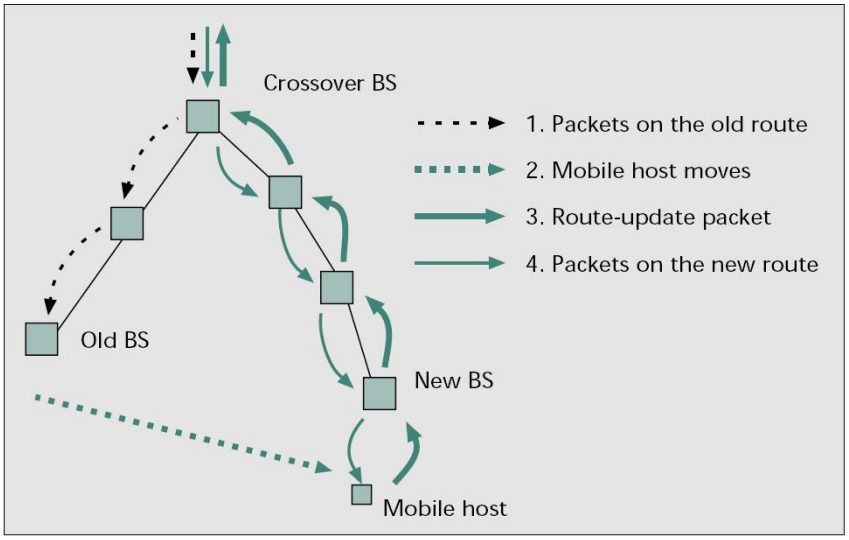

Figure 2.7: CIP handover [11]

CIP has implemented new important characteristics like paging increase the scalability, the autonomy of the mobile nodes and the way to maintain the state of the actives MNs using only simple IP packets.

2.4.3 - HAWAII

Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [9][12] is another complement to Mobile IP. It provides transparent mobility inside HAWAII domains but mobility between different HAWAII domains still uses MIP. Because it is transparent to MIP clients, they don't need to change, and HAWAII is only implemented in the other nodes of network. That allows that when MN moves between FAs in the same domain the handover is considered as local.

HAWAII domains have a gateway called Domain Root Router that connects to other domains. APs have HAWAII routing, but the MN only has one mobility protocol (MIP). This HAWAII routing is similar to CIP routing, where each router only has (in its database) the information about what is the next hop and is the chain of those database

entries that makes the route. The biggest difference is that here the route is always the shortest path and it is not need to pass through the gateway.

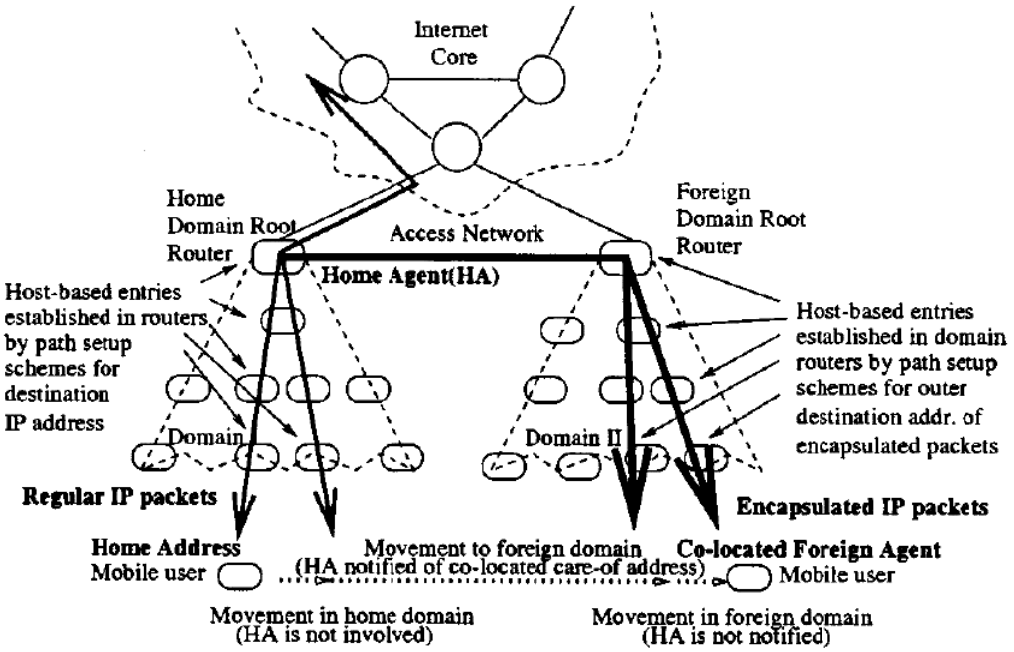

Figure 2.8: HAWAII Domain Hierarchy [12]

When a MN enters in a foreign domain for the first time, it is MIP that controls the handover, using the habitual entities: HA, FA and CoA. If the MN moves in the same domain between APs, it detects the new location using MIP mechanisms and sends signaling messages to Foreign Agent, trying to register the new location with the Home Agent. However, the FA, when receiving this message, verifies that MN didn't change the domain and so there is no need to inform the HA about the new location since it maintains its domain, Instead this information is used to create new entries in the routers database, to form a new route between the new AP and the FA that quickly restores connectivity.

The HAWAII routing is better than CIP but since it is only a transparent mechanism, it doesn't introduce new functionalities like paging or easy refreshing of the database.

2.4.4 - NetLMM

The Internet Engineering Task Force (IETF) suggested that, in opposition to the standardized host-based mobility management protocols that already exist, it would be desirable to have a localized mobility management protocol in which the host is not involved. So a working group called Network-based Localized Mobility Management (NetLMM) [13][14] was created, that lead to the as Proxy Mobile IP (PMIP) protocol that intends to be a mechanism where the MN doesn't need to implement nothing new in its IP stack, and do not change its IP address when moving to a new access router.

In NetLMM there are domains called Localized Mobility Domains (LMD) containing Access Routers (AR) that provide IP connectivity to the users and can manage one or more IP links, each one associated with at least an IPv6 prefix.

If the MN maintains or makes handovers between ARs of the same LMD it can keep the same IP address, because the prefix of the network is the same. When a mobile node moves and attaches to a new AR, (designed Visited Access Router (VAR)), the previous AR where it was attached, (named Home Anchor Router (HAR)), ensures the proper routing and forwarding of the data through a bidirectional tunnel between HAR and VAR.

When the mobile node connects to a LMD in the first time, it gets an address topologically correct, belonging to the network prefix, announced by the AR on the visited link, which allows it to communicate with any other node, using standard IP routing. When the MN moves to another link, changing the default router, it only needs to attach to a new link using usual procedures, as DHCP or Neighbor Discovery. It is the AR that detects if a new host has attached to the link and what was the previous IP address it was using. This router acts as VAR and sends a Location Update (LU) to HAR that bind and saves, in Location Cache, the addresses of mobile node and VAR, replying with a Location Acknowledgement (LA). From now on, the HAR starts to intercept the packets to host and

sends them to VAR, through a bi-directional tunneling. In the next movements of MN the HAR also needs to inform the old VAR that the mobile node has move to another AR, with a Move Notify message (see figure 2.9).

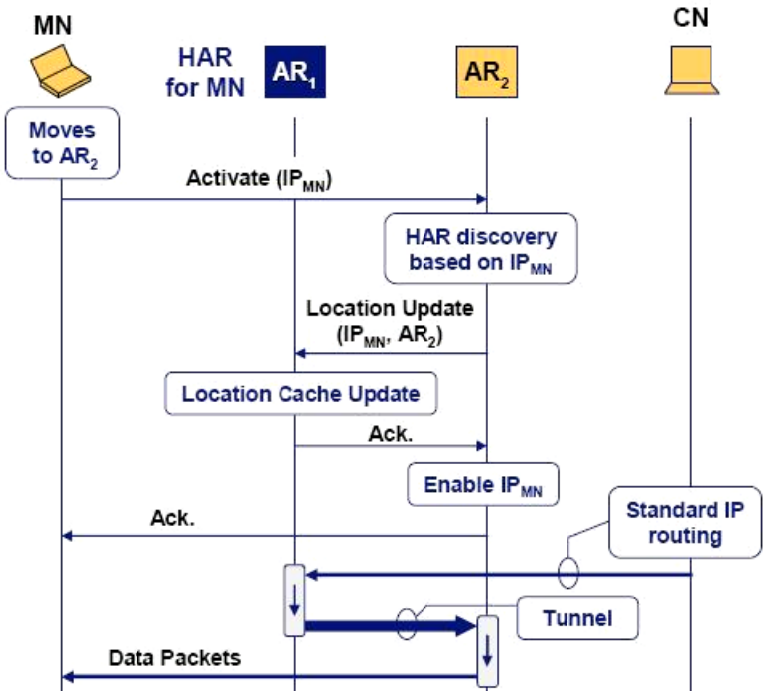

Figure 2.9: Data flow of MN's Handover using NetLMM [13]

This proposal minimizes the signaling in the wireless link, because it is almost between ARs without involving the host and without passing to wireless link.

2.5 – Inter-domain mobility

On the previous section we discussed methods to move inside an administrative domain of a network. For that we have some protocols as the well known Mobile IP, Fast Mobile IP or Hierarchical Mobile IP. Besides that, there are different proposals as CIP, HAWAII and NetLMM that already divide the mobility in local and global aspects, increasing the handover performance.

However the research in this field still continues and now it starts to appear some inter-domain proposals.

2.5.1 – MIFA

The Mobile IP Fast Authentication (MIFA) protocol [20] supports fast inter-domain mobility when integrated with other micro mobility protocol, and reduce handoff latency and the number of dropped packets when compared with MIP.

The biggest improvement is that FA is the one that makes the authentication, instead of the HA as usually. So the MN sends a Registration Request (RegRqst) to FA, that responds with a Registration Reply message (RegRply). When the MN receives this message it can resume transmission in uplink and, for downlink, a tunnel is established between the previous FA and the new one to forward packets until the HA is informed and creates a tunnel to the new FA. This way, the delay in communication between FA and HA is hidden from the application.

The local authentication is based on groups of neighboring FAs, where each FA defines its own FAs neighbor group, called Layer3-Frequent Handoff Region (L3-FHR). This L3-FHR contains the FAs to where the MN may move in the future, and have a security association with them.

The initial registration occurs as in the next steps and represented in figure 2.10.

The MN moves to a new domain and registers like in MIP, sending a RegReq message to the discovered FA, but in this message it indicates that prefers to use MIFA in the next registrations. Then FA sends the message to its Gateway Foreign Agent (GFA) who encapsulates it in an AAA-Mobile Node Request message (AMR) that sends to the AAA server of the Foreign domain (AAAF) including the suitable extension defined in AAA protocols to a FA-HA session key request. Now the AAAF sends the message to the AAA of MN's home domain (AAAH), who generates a MN-FA and a FA-HA session key that

defines the security association between them with an AMR message, in a Home Agent MN Request message (HAR) sending it to HA. By its turn, the HA extracts the session keys and RegRqst from the message and processes it using MIP. Then it encapsulates the session keys and a RegRply message in a HA MN Answer message (HAA) sending it to AAAH, that builds a AAA-Mobile Node Answer message (AMA) and forwards it to the AAAF server. The AAAF generates another set of FA-HA and MN-FA keys, which defines the security association between the HA and the new GFA to where MN may move, and between MN and the new GFA, respectively. It also generates the random variables used for authentication purposes in the future registration. Then it encapsulates everything in an AMA message and forwards it to GFA, which extract keys and send RegRply to FA that forward to MN.

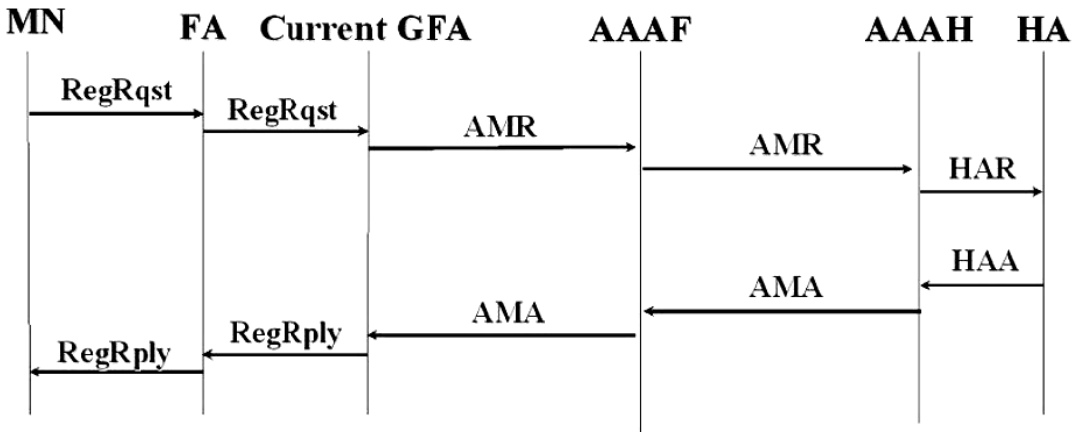

Figure 2.10: MIFA initial registration [20]

There is a need of distributing MIFA information from the present FA to other FAs that belong to different GFA, in order to allow a future move of the MN, as show in figure 2.14. This information distribution starts with a Move Probability Notification Message (MPNot) from GFA to the HA, which contains the FA-HA keys and the random variables. This will be used by the HA to built two authentication values, and include all in a Movement Probability Acknowledgment message (MPAck), that after authenticated with

the correct key, will be send to current GFA. In its turn, the current GFA distributes the information to the GFAs in the current L3-FHR. If there is security association between the current GFA and the other in L3-FHR, the GFA sends a MPNot message to each GFA, if there isn't security association between them, it's necessary to build one using AAA servers in a process similar as in the initial registration and represented in Figure 2.11.

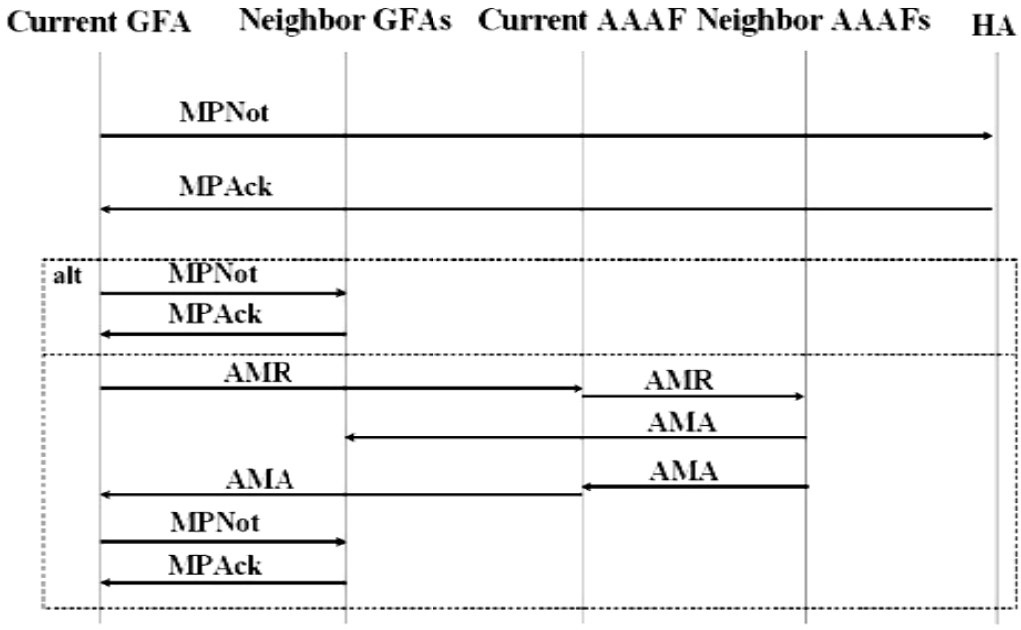

Figure 2.11: MIFA information distribution [20]

When the MN moves to a new domain, with a new GFA that is part of the L3_FHR of the previous FA, it could register using MIFA procedures. For that it needs to send a RegRqst message to the new FA that will forward it to the new GFA. This GFA checks the authentications, the MIFA information and the requirements requested from the HA using the information received before in the MPNot message and, if it's ok it sends a notifying message to the previous GFA to start forwarding traffic to MN through the new GFA. It also sends a RegRply message to FA, containing a new MN-FA key and two new random variables. This RegRply message is forwarded by the FA to the MN and, after it reaches the mobile node, can resume the transmission in uplink. GFA still generates another new FA-HA key introducing the security association between the HA and the new GFA, to where MN may move, and sends it with the two random variables to HA in a HA

Notification message, informing the new binding, to allow that HA established new tunnel between HA and the new GFA. It also sends a HA Acknowledgement message (HAAck), which contains two new authentication values built with random variables, to GFA.

Using this signaling (represented in figure 2.12), the time required to inform the HA and to established a new tunnel is hidden from the application.

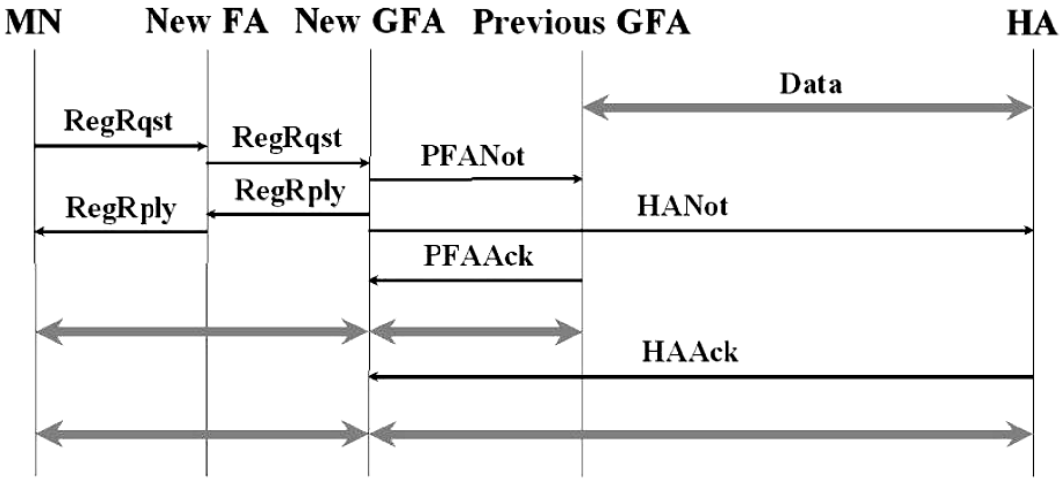

Figure 2.12: MIFA fast handover [20]

2.5.2 – Forwarding Router Discovery

The Forward Router Discovery proposal [21] introduces a new scheme that minimizes the redundant routing existent during a process of inter-domain handover, and that causes packet misordering and excess bandwidth consumption, using forwarding routers (FwR) discovery and proactive handover.

A Forward router is a router that buffers and redirects packets to NAR. A Cross over Router (CoR) is the best place to buffer packets because is where the routing path from CN to PCoA diverges from the routing path from CN to NCoA. The CoR can change

from one handover to another so each FwR is searched for each handover. This work is done by the PAR that searches FwR candidates, en route from CN to itself as en route from itself to NAR, compares them and chooses the common and most upstream, just before the MN starts the handover. If there wasn't found any common router the PAR acts as FwR.

The FwR discovery, from PAR to NAR, is made through the sending of FwR discovery messages from PAR to candidates to future NAR. These packets pass by FwRs candidates that insert its IP address inside the message, that forward to next hop until it reaches the NAR that replies with a FwR advertisement that contains the IP address of the FwR candidates, as in figure 2.13.

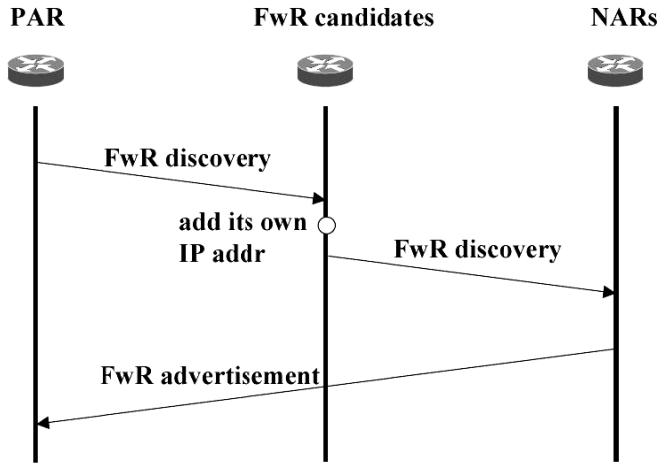

Figure 2.13: FwR discovery en route from PAR to NAR [21]

The FwR discovery, from CN to PAR, is more efficient and easy if the CN had specific features and sent FwR advertisement message to PAR, but if it doesn't have the necessary features it could be done in the previous handover when the present PAR was a NAR using Binding Updates (BU) and Binding Acknowledgement (BA) to pass the IP address of FwR candidates. Figure 2.14 illustrates this discovery, where the present PAR is called ŃAR.

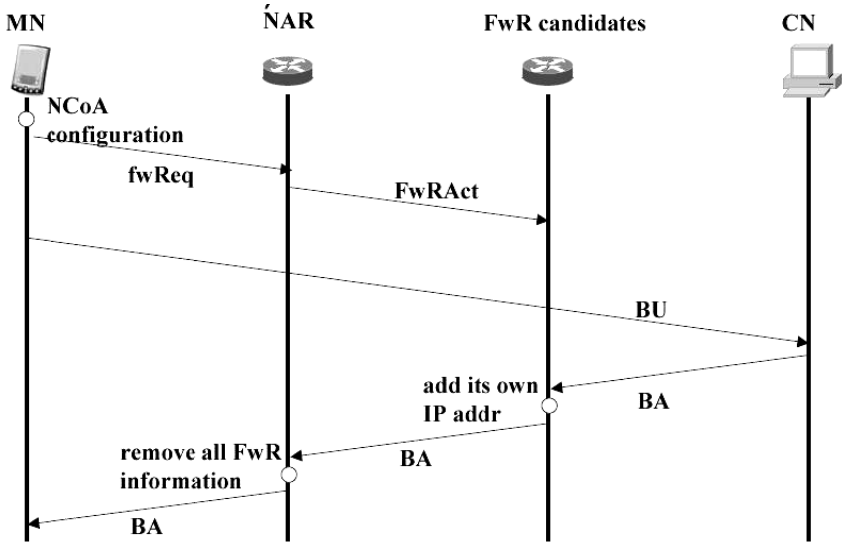

Figure 2.14: FwR discovery en route from CN to PAR [21]

The Proactive Handover (figure 2.15) is divided in two parts: the Proactive packet buffering and the packet forwarding.

The proactive packet buffering avoids the lost of packets, using buffering in the FwR. It begins with a buffering request message sent from the MN to the PAR, where the mobile node includes the new AP identifier that will allow PAR to know the address of NAR. The PAR sends the message to the chosen FwR candidate, who starts replicating packets sent from CN to MN, forwarding the originals and buffering the others.

The packet forwarding part starts when the MN sends an fwReq message to PAR, instants before breaking the connection, that is forwarded to the proper FwR and when reaching the destination, the FwR starts forwarding packets from CN to PCoA to NAR preceded by the previously buffered packets. By its turn, the NAR receives the packets and starts buffering them. After the MN connects in a new network it sends a fwReq message, this time to NAR, that starts forwarding packets sent by FwR, preceded by the previously buffered packets.

With this mechanism, redundant routing is avoided, and packet misordering, loss and bandwidth waste suppressed.

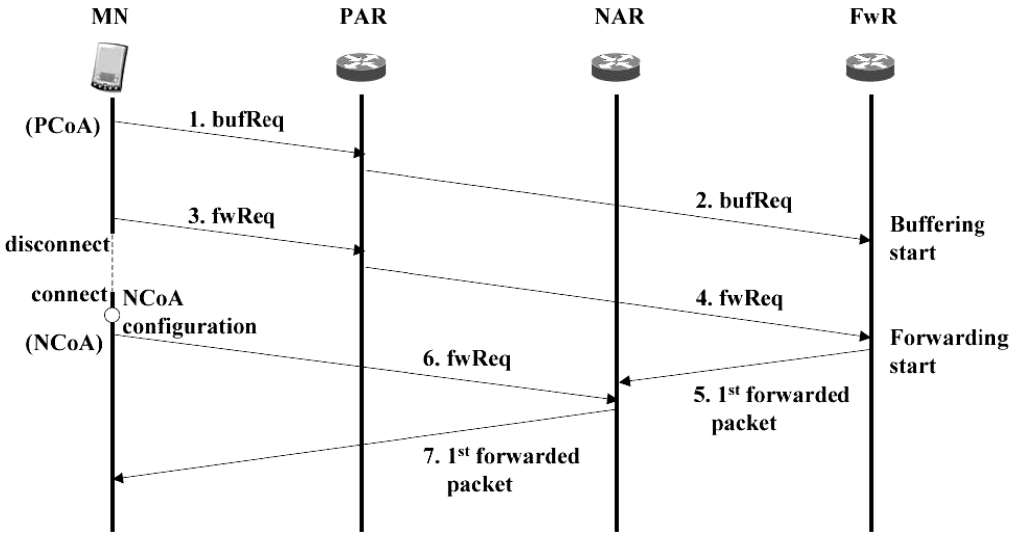

Figure 2.15: FwR Proactive Handover [21]

2.5.3 – SIP

In November of 2000, the 3rd Generation Partnership Project (3GPP) accepted Session Initiation Protocol (SIP) [15][16][17] as a signaling protocol and a permanent element of the IP Multimedia Subsystem (IMS) architecture, for IP based streaming multimedia services in cellular systems. The IMS is an architectural framework for delivering internet protocol multimedia to mobile users.

With 3GPP and other one, like 3GPP2 or MWIF (Mobile Wireless Internet Forum), agreeing that SIP is one of the bases of the session management of the mobile Internet, it seems that SIP will certainly be an integrated part of the mobile Internet's protocol architecture. SIP has other advantages in mobility support, like providing a mean of route optimization and improving performance for real-time services, handling mobility at a semantic level, above the IP terminals.

A user in SIP is an entity that associates with a particular domain. So if a roaming user is in a foreign domain, different from its home domain, the traffic of signaling must pass through its home proxy server. If the two domains are far away, the delay caused by the triangular route through the home domain, is not acceptable for time sensitive

applications. It was proposed to abstract the actual identifier, eliminating per-call coordination to minimize the signaling traffic, which is done in Handle SIP (H-SIP).

H-SIP allows that users can identify each other, as well as the SIP servers they are associated with, using handles instead of URIs and domain names respectively. URI is the Uniform Resource Identifier used in common SIP to allow location independence and personal mobility. Handle is a persistent name that can be associated to a set of attributes that can describe locations permissions, administrators and state. With this, it can be created an abstraction that allows the system to route calls independent of user location and domain association. As each user has its own handle and administrates it, the user can chose the rights of the other handles over him and includes also the handle of any proxy server that it wishes to register, no matter what domain it belongs.

To the authentication, the user needs to provide credentials to the local server which validates it against the Handle System. Saving passwords on user handle avoids the internal accounts on proxy server, makes the credential valid for all realms, provides the correct administrative privileges and allows that an authenticated SIP message travels for multiple domains, without the need of re-authentication in each domain of the message path.

After authenticating and registering with the foreign server, the user allows corresponding users to reach him by simply addressing it name.

2.6 – Mobile operator's federations

Different domains are usually owned by different companies, perhaps competing companies like Internet Service Providers (ISP) or Mobile network operators. This is a problem for inter-domain mobility because these companies do not want to exchange

information and administration control between them. One solution developed in the project DAIDALOS is to use federations, and that is the same solution that will be used in this work.

Federation is an agreement between different domains where they decide the level of trust and the type of information they give to other administrative domains; it addresses also as the interoperation between domains, which is how the information is exchanged using determined type of packets and policies of communication. It is the federation type that decides the AAA [22] (Authentication, Authorization and Accounting) protocol that will work between the two domains. The Authentication is the process where one entity establishes a unique digital identity. Authorization is the act of granting some privileges, or not, based on permissions of that identity. Accounting has to do with the consumption management, planning and billing the network resources by some identity.

There are five classes of federations in DAIDALOS [19] differing in the relationships between the domains.

- F-Class 1 is when there is no interaction between domains. The user needs two separated contracts and has two bills in the case of domains belonging to different providers.
- F- Class 2 is the basic roaming model and the most common configuration in mobile network operators. The user has one contract and one integrated bill and the two domains are able to minimally interoperate in the sense of an exchange of accounting and charging information.
- F-Class 3 is considerate as personalized roaming, because besides the information shared in basic roaming there is a transfer of personalization information like user profile.
- F-Class 4 is a Premium roaming model with a great level of cooperation between domains. Session continuity across domain boundaries needs to be guaranteed and the Service Level Agreement (SLA) between the user and the operator must be fulfilled also when in roaming, and needs context information exchange because most running sessions imply stored state that must be moved between the two domains.

- F-Class 5 is the highest class for federations and is a fully federated environment. It seems for the user that it makes an intra-domain handover instead of an inter-domain, because all information can be exchanged between the two domains. Note that some policies implemented between domains have to be respected; for example, all signaling information is only exchanged between determined special nodes and not between all.

Chapter 3

Eppur Si Muove

3.1 - Introduction

ESM (*Eppur si muove,* [18] that means *And yet it moves*) it's a proposal of the Heterogeneous Networking Group (HNG) of the Instituto de Telecomunicações – Pólo Aveiro (IT-Av) to define a complete and efficient mobility architecture entirely operated by the network, mostly without intervention from the terminal, with support for multihoming and Quality-of Service. The preference to avoid terminal intervention has the benefit that signaling is faster, since the core signaling is faster, congestion-free and consumes no resources of the wireless medium.

A main concept in ESM is to achieve terminal mobility in a location independent fashion using a flat IP addressing namespace (hence, supporting locator and identifier decoupling). The using of flat IP on the architecture could be complicated since global routing is based on address prefixes, in order to reduce the size of routing tables, but it brings many advantages. Initially, terminals acquire an IP address consistent with the location in the network where they are, but then they could move to anywhere that there is no need of re-configuring, so the IP address continues the same and mobility is very easy for them. This enables the IP address to act like an identifier and not as a locator, beneficiating the privacy of the user. However it could be used to identify its home domain when in foreign domains. Legacy applications can still be used in ordinary processes, such as routing and subnetting, since this addressing scheme fits the currently used.

To solve the problem of finding the location of a node, ESM uses a central repository (LS, location services) that maintains an entry for the topological position of every node.

ESM could be used in intra-domain and inter-domain with some minor differences in architecture, as we'll discuss.

3.2 – Intra-domain ESM

In the intra-domain model we have a LS (location service) that maintains a database with the topological position of every mobile node, and edge nodes (EN) or entry nodes, which receives packets from other domains like border routers or from end-users like access routers.

When an edge node intercepts a packet for MN, it checks if the destination IP has the same prefix of the domain where it is. If not, it forwards the packet by normal routing. If yes, it searches, in its cache, the location of the mobile node and if doesn't have it, sends a message to the LS that will reply with the IP address of the AR where the MN is attached. Once the location is known, EN includes a new routing header in the packet, where it fills the Precedence Address (PA) field with its own IP address and the Transit Address (TA) field with the IP address of the AR where MN is connected. After this, the packet is forwarded to the correct AR using normal routing, passing through core routers that aren't aware of mobility, and when it arrives to the destiny AR, it will be stripped of routing headers and delivered to MN. This is shown in figure 3.1.

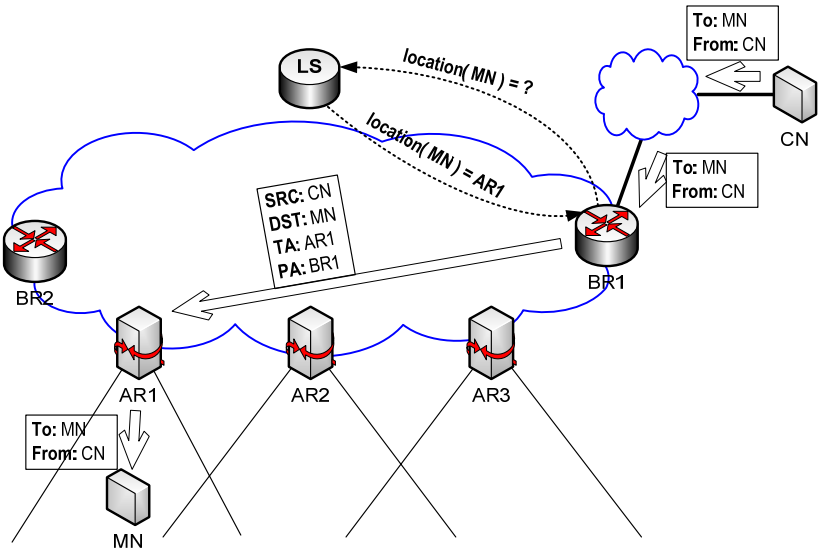

Figure 3.1:ESM: intra-domain packet delivery [18]

A Handover is processed in several steps (illustrated in figure 3.2):

- The terminal disconnects from current AP (pAP) and connects to a new AP (nAP).
- Immediately it initiates a L3 connection to the new AR (nAR), using Neighbor Discovery Protocol (NDP), and sends a Router Solicitation Message (rtSol) with its IP address, its L2 address and some authentication token. At this time, the MN doesn't know the IP or L2 address of nAR.
- nAR receives the rtSol, the ESM takes control of handover and sends an update message to LS.
- The LS checks the terminal profile and sends a update acknowledge message to nAR with its specific policies. It also sends a signaling message to the pAR to inform the new location of the MN.
- Once the pAR is informed about the location of MN it starts to transfer context that is needed to reestablish any ongoing sessions (QoS sessions characteristics, peers locations with which the terminal is communicating, etc) to nAR. It also receives the packets that are destined to MN, checks its origin (looking to PA in the source routing) and updates the edge nodes that forward them. This way the ENs receives the update and starts forwarding to nAR.

- Finally nAR sends a Router Advertisement message to the MN informing that it can start receiving and transmitting packets.

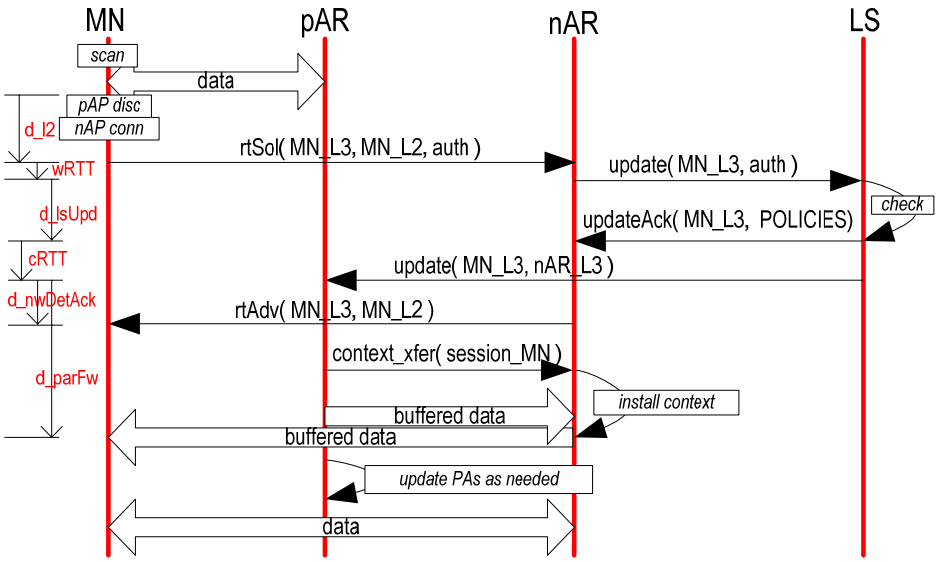

Figure 3.2: Handover signaling [18]

3.3 – Inter-domain ESM

3.3.1 – Inter-domain scenario

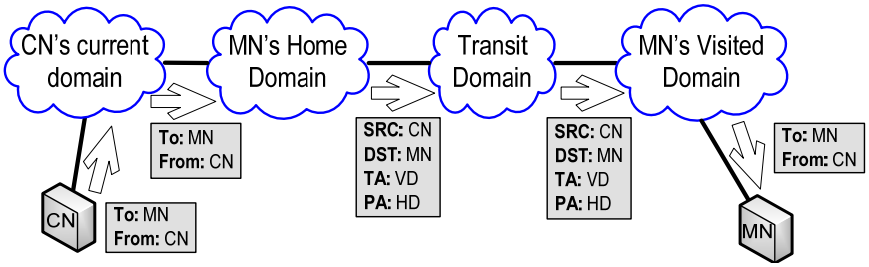

Figure 3.3: Inter-domain mobility scheme [18]

In the inter-domain mobility architecture, the elements of the ESM in intra-domain architecture (LS, edge routers, nAR, pAR, MN, etc) are maintained as well as almost its functions, but there are some differences in the delivery of packets and in the way signaling in a handover is done.

When a packet is sent by CN to MN and passes by one edge router, the IP address of the destination is checked. If it belongs to other domain the EN forwards the packet using normal routing, otherwise, the edge router needs to look into its cache, searching for the location of mobile node or query LS about it. If the location is in the same domain of EN, it forwards the packet using normal intra-domain architecture; if the location points to other domain it will be used the inter-domain ESM.

In the ESM's inter-domain architecture, if the MN is in a visited domain and the EN belongs to the home domain, when a packet arrives to it, the information in the cache of EN or retrieved by LS is the IP address of the nAR that serves MN in the Visited Domain (VD), the domain where the MN is connected. So EN includes a routing header, fills it using the IP address of nAR as TA adds its own IP address as PA and forwards the packet by normal routing.

When a Handover occurs, the signaling is very similar to the above description, with the difference that here exist two Location Services, instead of only one, communicating and sharing signaling between them. So the handover can be summarized in the following steps:

- Terminal disconnects from current AP in one domain and connects to a new AP in other domain.
- Immediately it initiates a L3 connection to the nAR and sends a Router Solicitation Message with its IP address.
- nAR receives the rtSol and sends an update message to LS of the Visited Domain.
- LS of VD checks the terminal profile and detects if the MN belongs to other domain, which is identified by the prefix of the terminal's IP address. It sends a message

to LS of the HD informing the new location of the MN and the IP address of nAR, and sends other message to nAR with MN's specific policies.

- LS on HD receives the message from LS on VD and sends a new update message to pAR informing the nAR where MN is attached.
- Once pAR is informed about the location of MN, it starts to transfer context to the nAR, sending it to the LS on HD that forwards to LS on VD. This in its turn, forwards to nAR, it also receives the packets that are destined to MN, checks its origin and updates the edge nodes that forward them. This way the ENs receives the update and start forwarding to nAR.
- nAR sends a Router Advertisement message to the MN informing that it can start receiving and transmitting packets.

3.3.2 – inter-domain optimization

The ESM architecture proposed above was further extended in order to improve the inter-domain scenarios. There are some proposed ideas to make inter-domain ESM architecture work.

When the mobile node is in a Visited Domain, the Border Routers can be updated by the pAR, with the destination of the nAR, as it is done in intra-domain. This is the simplest solution because then, after being updated, the Edge Node from Home Domain inserts the routing headers in the packet with the VD's AR IP address that serves MN and then forwards the packet directly to it, which then takes of the routing header and delivers it to MN. But this brings some problems, like scalability. Using this method, the Home Domain needs to know every nAR from other domains where MNs were attached. In the case of several MN from HD in the same Visited Domain, LS needs to have a lot of nAR IP address in its database. One solution to this problem is to give to Home Domain the information about in which Visited Domain is the MN and the VD control de rest.

Other problem is that, in the ESM proposal, when a MN makes a handover between two ARs of the same visited Domain, the LS of the HD needs to be updated. In other words, every time MN makes a move, the LS of its Home Domain needs to receive and send signaling which is unnecessary. If the message that the LS of the Visited Domain sends to HD's LS includes an identifier of the visited domain, instead of only the nAR, the packets will start be forward to VD, by the BR on the HD. Then when intercepted by any BR of the VD it they will be forwarded to the correct nAR. With this approach the only entities that know the exact location of the MN are the elements of the domain where it is.

The update of the BRs by the pAR could be a problem too when MN moves between ARs inside a visited domain. When this happens, pAR can't send updates directly to BRs in the Home Domain because they are in different domain and couldn't exist any administrative signaling between them if this didn't pass through both LSs. To solve this without charging the communication between LSs, every time a HD's BR needs to know the location of the MN, it could be sent as an update message in multicast to a group of BR of the domain. Instead of having pARs updating Edge Routers is the LS that do the updates. When it receives the information message, about the nAR and the domain that serve MN, sends an update message to all its Edge Nodes, using multicast to informing about the domain where MN is, in the case that the ENs belongs to HD, or informing about the nAR, in the case that the ENs belongs to VD. If that handover is done with an ongoing flow of traffic, there is no need to wait for the message from pAR because the message will be received automatically.

The same problem, with administrative agreements, exists when the pAR needs to transfer the context to the nAR but this time since it causes a small traffic (only during handover execution), it could be done using the route between LSs (pAR sends to its LS that sends to VD's LS that delivers to nAR).

Chapter 4

Architecture Evaluation

4.1 – Network Simulator -2

To simulate ESM we used the Network Simulator 2 software. (NS-2)

NS-2 is a very powerful tool, one of the best in the usual simulators for networks and gives substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It is a discrete event simulator, target at networking research, consisting of many modules that worked together and allow changes to what is needed. But isn't so simple to simulate the ESM in NS-2.

In NS-2, we created a new type of packet, named ESM, and its correspondent headers, to identify the signaling packets and to allow a new routing header in the normal packets, which is necessary to ESM routing. It was also needed the creation of some functions that determine when the handovers were made, and sent of the rtSol message that NS-2 didn't have. It was also necessary to transform the behavior of some nodes to act like the elements of the ESM architecture.

In the case of networks wired and wireless links it's needed to use a special node called Base-station (BS). A BS is a node that makes connection between the wireless part and the wired part, is a kind of mix between an access router and an access point. However, the use of BSs implicates the use of hierarchical address in the wired part. This means that flat IP doesn't work and when a terminal moves to another sub-network the routing still sends the packets to the previous place where it was, because in hierarchical routing, each node only knows about the other nodes in the same level. So it was needed

to force them to allow that the terminal wandering through all BSs receives packets as usual.

To do this we worked with Classifiers. A node in NS-2 has many different types of classifiers, each one looks at a specific portion of the packet forwarded through the node and has a function according to that portion. So it was needed to detect the classifiers where we can change the way the hierarchical routing works, without changing the entire routing protocol, to allow that MNs can receive packets everywhere they were.

DSDV (Destination Sequenced Distance Vector) has been tested and discarded because it takes too much time to converge after every Handover, due to the MNs having different prefix of location, so it was chosen a recent NS-2 routing protocol, NOAH (NO Ad-Hoc) for wireless part, since it is the only protocol that works for wireless in NS-2 that is not an ad-hoc protocol. This is a very simple protocol that sends packet from MN to the BS that was defined to serve him, that if it is in the range it will be deliverable and the same to traffic from BS to MN.

There were other emulations that were made, like the detection of a MN by the BS, that don't exist in NS-2 and the virtual separation between two different domains that in NS-2 were the same.

4.2 – Simulation scenarios

4.2.1 – Intra-domain simulation scenario

In the simulation the intra-domain architecture presented in section 3.1 is extended from the one that was been proposed by HNG, as referred above. In the delivery of packets it is equal as the initial proposal.

When an edge node intercepts a packet for MN, it checks if the destination IP has the same prefix of the domain that it is in: A) If not, it forwards the packet by normal

routing; B) if yes, it searches in its cache the location of the mobile node. If it doesn't find it, sends a message to LS that replies with the IP address of the AR where the MN is attached. Once the location is known, EN includes a routing header where it fills the Precedence Address (PA) with its own IP address and the Transit Address (TA) with the IP address of the AR where MN are connected. After this, the packet is forwarded to the correct AR using normal routing and when arriving to the destiny AR, it will be stripped of routing headers and delivered to MN.

The handover signaling in the simulation has some pragmatic differences:

- Terminal disconnects from current AP (pAP) and connects to a new AP (nAP).
- Immediately it initiates a L3 connection to the new, and sends a Router Solicitation Message (rtSol) with its IP address.
- nAR receives the rtSol and sends an update message to LS .
- LS checks the terminal profile and sends an update acknowledgment message to nAR with its specific policies and a update message to pAR to inform the new location of the MN. It also sends in multicast an update message to the group of Edge Nodes, reaching like that to all EN, with the IP address of the nAR where MN is attached
- Once pAR had been informed about the location of MN it starts to transfer context that is needed to reestablish any ongoing sessions to nAR.
- Finally, after context is installed, the nAR sends a Router Advertisement message to the MN informing that it can start receiving and transmitting packets.

4.2.2 – Inter-domain simulation scenario

In the inter-domain mobility architecture that was chosen to simulate, the elements of the ESM in intra-domain are still maintained, as well as almost all its roles. Some difference were: HD's EN fills TA in the routing header with one IP address that

identifies the VD and not with the IP Address of the nAR; and the EN are update by receiving a multicast message from LS and not from pAR.

When a packet is sent by CN to MN, and passes by one edge router, it checks the IP address of the destination. If it belongs to other network, it forwards the packet using normal routing. If it belongs to the network where it is, the edge router needs to look into its cache searching for the location of mobile node or query the LS about it. If the location is in the same domain, it forwards the packet using normal intra-domain architecture. If the location points to other domain, it will be used the inter-domain ESM. So the EN includes a routing header, fills it using the IP address that identifies the visited domain as TA and its own IP address as PA, and forwards the packet.

When the packet arrives at a border router of the VD, this identifies the forward packet looking to the TA and strips it finding the MN's IP address. Then it searches the topological location of mobile node, finding the IP address of the AR that serves the MN, and use it as the TA in the new source routing (without forgetting its IP address as PA) and forwards the packet to AR that strips it and delivers to MN as in intra-domain architecture.

The registration signaling can be explained in the next steps:

- Terminal disconnects from current AP in one domain and connects to a new AP in other domain.
- Immediately it initiates a L3 connection to the nAR and sends a Router Solicitation Message with its IP address.
- The nAR receives the rtSol and sends an update message to LS of the Visited Domain.
- The LS of VD checks the terminal profile and detects if the MN belongs to other domain, which identifies by the prefix of the terminal's IP address. It sends a message to LS of the HD informing the location of the MN and the IP address that identify Visited Domain. It sends also an update message to the multicast border routers group sharing information about the MN for all BRs and sends one more message to nAR with MN's specific policies.

- LS on HD receives the message from LS on VD and sends a message to boarder routers multicast group of its domain with the information of the network's identifier IP address where MN is. It also sends other message to pAR informing the new network where MN is attached.
- Once pAR had been informed about the location of MN, it starts to transfer context to nAR, sending this to LS on HD that forwards to LS on VD, which in its turn forwards to nAR.
- nAR sends a Router Advertisement message to MN, informing that it can start receiving and transmitting packets.

4.3 Simulation

In the simulation we tested a simple topology to study the basic behavior of the ESM. Despite is simplicity, the topology allows understanding of the intra-domain and inter-domain architecture at the same time.

The fact that LS alerts every EN from its domain, could be, not the correct solution to this problem, but a possible solution for simulation and evaluation purposes. When the LS informs all the other elements of the domain about the changes with the MNs (inform nAR, pAR and all edge nodes) there will be too much centralization of information in only one node and one of the objectives of ESM is to spread and divide the administrative functions for the elements of the network.

With these adopted solutions in inter-domain architecture, the intra-domain ESM proposal needs to be reviewed to grant better compatibility between both. So despite the fact that in intra-domain pAR updates BRs when it is needed after the MN executed an handover, to make it more similar and a better implementation in the two aspects, in the simulation, it will be LS that updates every Edge Nodes sending a multicast update message to the group of edge nodes. This is needed because if they aren't adapted to

each other when a handover is made between ARs in a foreign domain, the two architectures could enter in conflict.

In NS-2 isn't possible to simulate different administrate domains so all of them are an F-class 5, meaning that they have an high degree of interaction. However, two different and symmetrical domains are distinguished in our simulation, each one containing one LS, one MN, one EN (in this case a BR), two AR/AP (since Base-stations emulate both together) and three other single nodes. The only connection with administrative control between them is between their LSs.

In general, there is a traffic flow from Correspondent Node (CN) to the Mobile Node (MN). There is a domain called Visited Domain, where CN is initially connected to BS0. The domain contains also LS1 and BS1. The other domain, called Home Domain, contains the MN initially connected to BS2, LS2 and BS3. The IP address that identifies the network, it's the same of the Border router, since there is only one route between domains. It was needed to put MN sending one message packet to the nAR after each physical handover to emulate the detection between APs and MN which didn't exist in NS-2, and that correspond to a Route Solicitation Message that is not an ESM signaling message, but a mechanism request by the network.

For testing the topology with a higher load in specific points, the delay between links was changed. Every wired node uses hierarchical routing as routing protocol and in the wireless links it uses NOAH protocol.

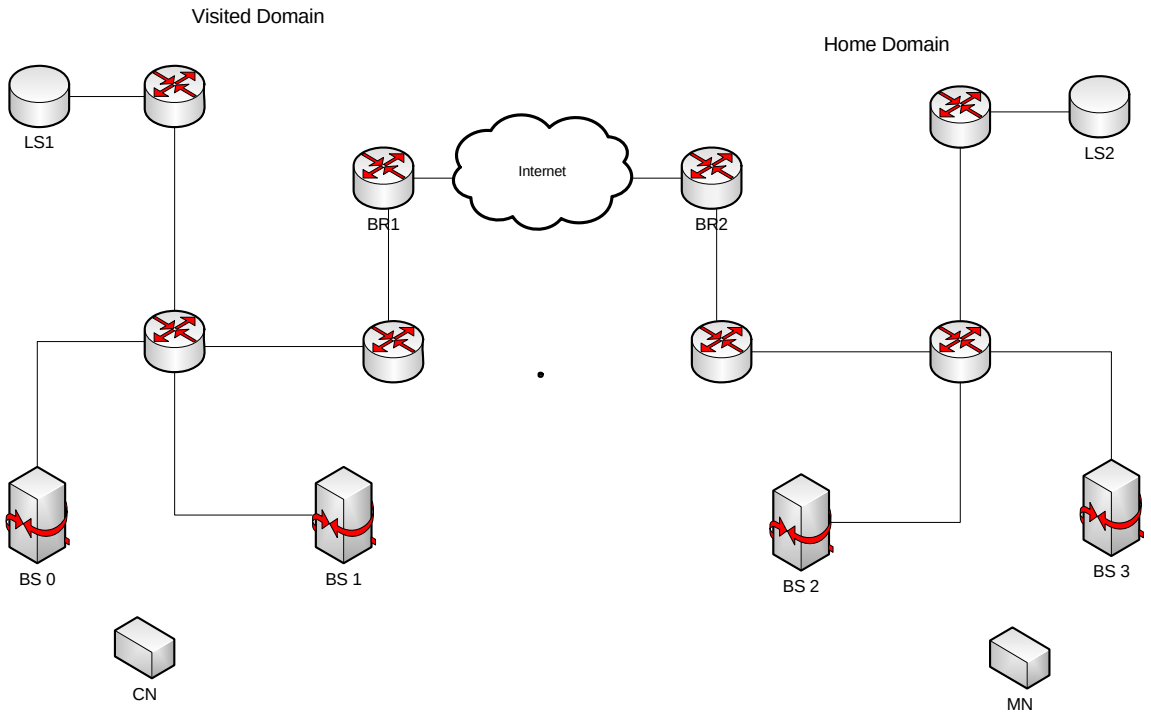

Figure 4.1: Simulation scenario

There were five handovers in the simulation, two intra-domain, two inter-domain and one intra-domain inside a foreign domain. The first HO is when CN moves from BS0 to BS1 (intra-domain) and is not much relevant from the study, because CN just sends packets. The second is MN moving from BS2 to BS3 (intra-domain), the third is when the MN moves from BS3 to BS0 (inter-domain), the fourth is the movement of MN from BS0 to BS1 (intra-domain inside a Visited Domain) and the fifth is when MN backs from BS1 to BS2 in its home domain. In simulations we used two types of traffic: UDP with Constant Bit Rate (CBR) and TCP over a FTP application. It were made ten simulations to each test.

All wired nodes have a 5Mb bandwidth and a delay of 2ms except the link between the two domains, that has 25ms of delay, or the cases where it was need to change these specifications to test the architecture. The rate of CBR is 256 kbps and the size of packets is 1000 bytes. The node moves very fast from one AR to another.

To simplify the presentation of results each handover was made at the same simulation time, in the different simulations.

The handover of CN between the BS0 and BS1 occurs at t=50s and is an intra-domain handover.

The handover of MN between the BS2 and BS3 occurs at 7=75s and is an intra-domain handover inside the Home Domain of MN;

The handover of MN between the BS3 and BS0 occurs at 7=100s and is an inter-domain handover from the Home Domain to Visited Domain;

The handover of MN between the BS0 and BS1 occurs at 7=125s and is an intra-domain handover inside the Visited Domain of MN;

The handover of MN between the BS1 and BS2 occurs at 7=150s and is an inter-domain handover from the Visited Domain to Home Domain;

4.4 - Results

4.4.1 – Handover duration

The messages of signalling registration are presented in the form *source-destination* where the source and destination are the sender node and the receiving node of that message, respectively. The MN-nAR is the Router Solicitation message; NAR-LS is the update message to LS; LS-nAR is the update acknowledge message; LS-BR and LS-pAR is the update information message to BR and pAR; and the nAR-MN is the Router Advertisement message to MN. There is also a pAR-nAR that represents the transference of context between the two ARs, and a LS-LS message in the inter-domain handovers that is the message between the two domains updating the position of MN.

4.4.1.1 – CBR Handovers

Figure 4.2 represent the duration of signaling packets in seconds during the handover of CN from BS0 to BS1 at 50s and the table 4.1 shows the times of the same packets.

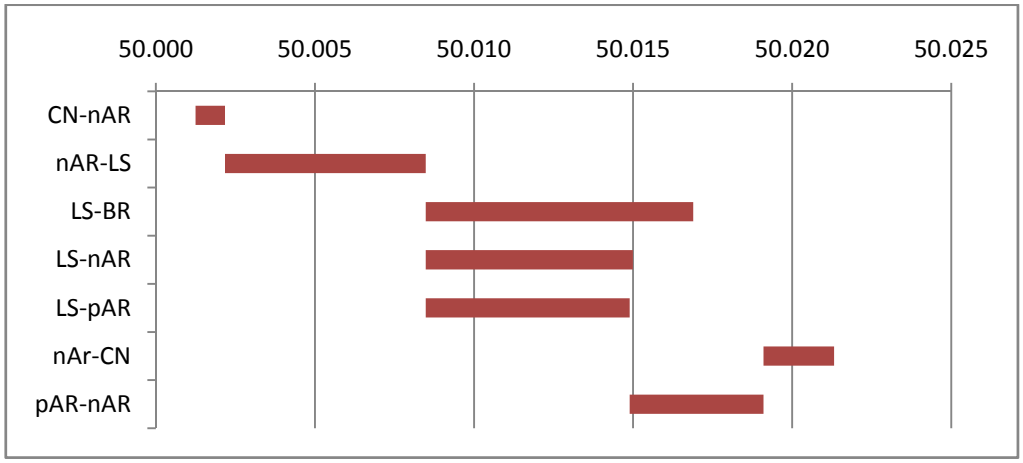

Figure 4.2: signaling packets duration 1st Handover, CBR

t0 = 50	initial time (s)	duration (s)	final time (s)
CN-nAR	50.00125	0.00093	50.00217
nAR-LS	50.00217	0.00631	50.00848
LS-BR	50.00848	0.00841	50.01689
LS-nAR	50.00848	0.00651	50.01499
LS-pAR	50.00848	0.00641	50.01489
nAr-CN	50.01910	0.00222	50.02132
pAR-nAR	50.01489	0.00420	50.01910
Handover reg duration		0.02007	

Table 4.1: signaling packets duration 1st Handover, CBR

In this case it's an intra-domain handover, where the node that made a movement was CN. The handover is very fast, with registration duration of 20ms, since the first signaling packet was send, and 21ms since the start of CN movement at 50s. This is the fast handover time was get in the different simulated handovers cause is the Correspondent Node who moves and this node only transmits packets in CBR mode what reduces the probably of some interference.

Figure 4.3 represent the duration of signaling packets in seconds during the handover of MN from BS2 to BS3 at 75s and the table 4.2 shows the times of the same packets.

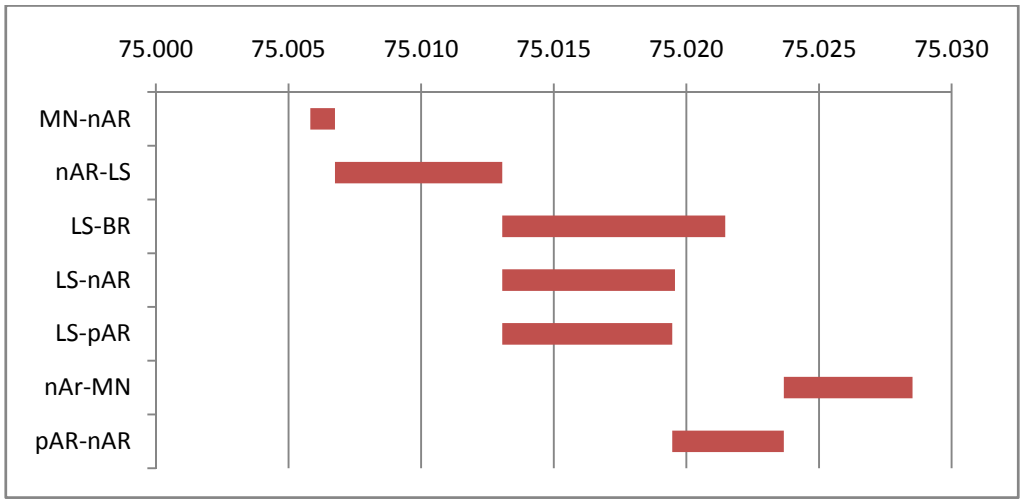

Figure 4.3: signaling packets duration 2nd Handover, CBR

t0 = 75	initial time	duration	final time
MN-nAR	75.00582	0.00093	75.00675
nAR-LS	75.00675	0.00631	75.01306
LS-BR	75.01306	0.00841	75.02147
LS-nAR	75.01306	0.00651	75.01957
LS-pAR	75.01306	0.00641	75.01947
nAr-MN	75.02367	0.00486	75.02853
pAR-nAR	75.01947	0.00420	75.02367
Handover reg duration		0.02270	

Table 4.2: signaling packets duration 2nd Handover, CBR

This is an intra-domain handover of MN. Its duration is a little higher than the intra-domain handover of CN. The duration of registration is 23 ms and the total duration since the beginning of the movement at 75s is 28.5ms. This time the mobile node that executes handover already receives packets and the first time packet received after registration was after 43.9ms from the start of handover.

Figure 4.4 represent the duration of signaling packets in seconds during the handover of MN from BS3 to BS0 at 100s and the table 4.3 shows the times of the same packets.

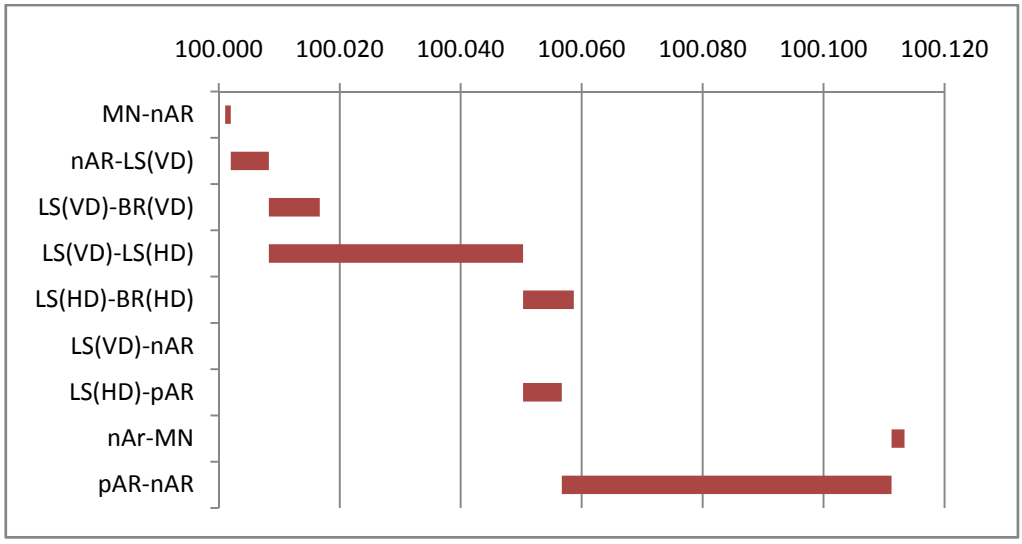

Figure 4.4: signaling packets duration 3rd Handover, CBR

t0 = 100	initial time (s)	duration (s)	final time (s)
MN-nAR	100.00105	0.00093	100.00197
nAR-LS(VD)	100.00197	0.00631	100.00828
LS(VD)-BR(VD)	100.00828	0.00841	100.01669
LS(VD)-LS(HD)	100.00828	0.04202	100.05031
LS(HD)-BR(HD)	100.05031	0.00841	100.05872
LS(VD)-nAR	100.00828	0.00000	100.00828
LS(HD)-pAR	100.05031	0.00641	100.05672
nAr-MN	100.11125	0.00212	100.11337
pAR-nAR	100.05672	0.05454	100.11125
Handover reg duration		0.11232	

Table 4.3: signaling packets duration 3rd Handover, CBR

These are the times of the inter-domain handover from the HD to the VD. The registration duration is 5 times longer than a registration in intra-domain, 112ms and the first packet of data received in MN was at 100.126s, this is, 126ms after the handover starts. However 96 ms (84ms+54ms) of the registration duration were spent in the packets that travel between the two domains (LS(VD)-LS(HD) and pAR-nAR). Besides that there are two more packet messages than in an intra-domain handover registration.

Figure 4.5 represent the duration of signaling packets in seconds during the handover of MN from BS0 to BS1 at 125s and the table 4.4 shows the times of the same packets.

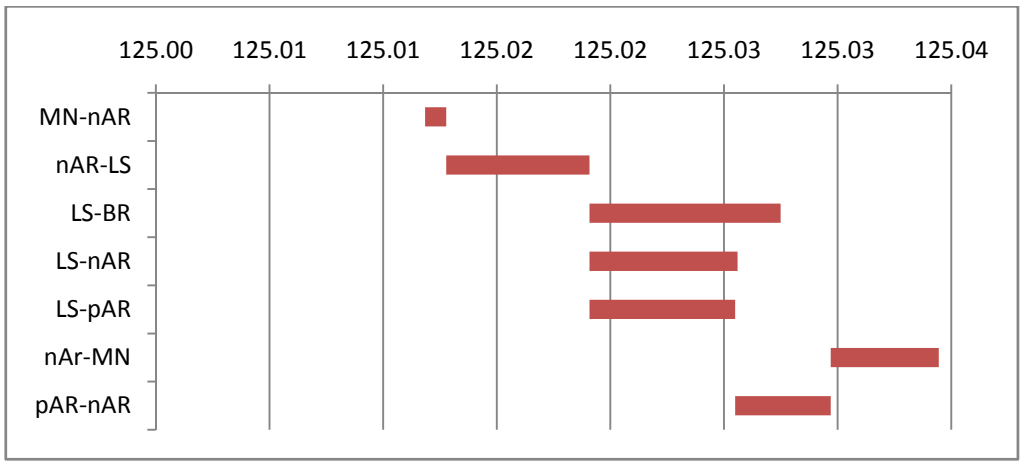

Figure 4.5: signaling packets duration 4th Handover, CBR

t0 = 125	initial time (s)	duration (s)	final time (s)
MN-nAR	125.01185	0.00093	125.01278
nAR-LS	125.01278	0.00631	125.01908
LS-BR	125.01908	0.00841	125.02749
LS-nAR	125.01908	0.00651	125.02560
LS-pAR	125.01908	0.00641	125.02549
nAr-MN	125.02970	0.00476	125.03445
pAR-nAR	125.02549	0.00420	125.02970
Handover reg duration		0.02260	

Table 4.4: signaling packets duration 4th Handover, CBR

These are the results of an intra-domain handover in a foreign domain, MN in the Visited Domain. The duration of registration is 22.6 ms, duration between the start of movement and the last packet of registration is 34.5 ms and the first packet received after registration was at 125.063 s. These times are very similar to a simple intra-domain handover and the only difference is that the MN and the CN are in the same BS which means half of the bandwidth to each that only affects the MN-nAR message that was sent later than usual.

Figure 4.6 represent the duration of signaling packets in seconds during the handover of MN from BS1 to BS2 at 150s and the table 4.5 shows the times of the same packets.

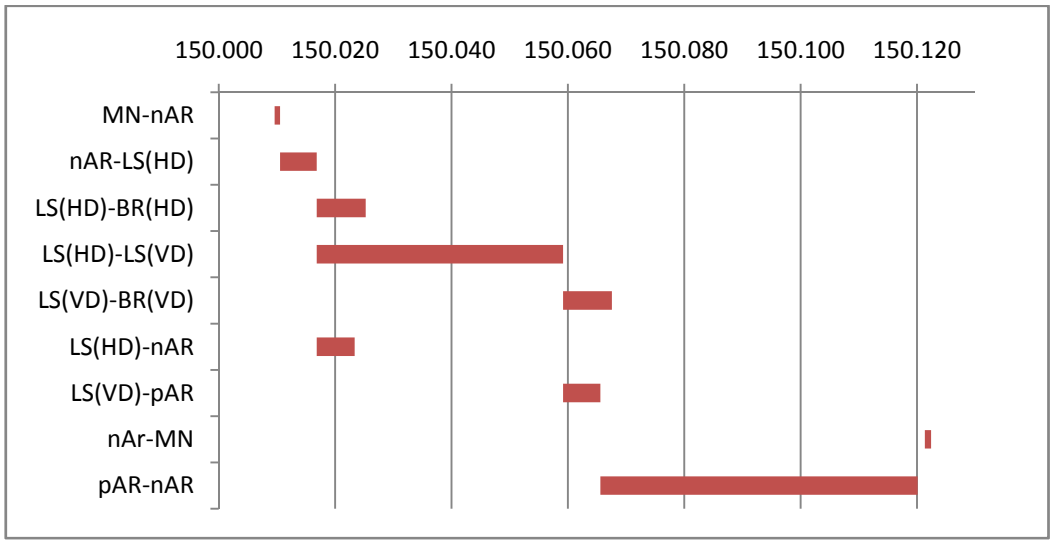

Figure 4.6: signaling packets duration 5th Handover, CBR

t0 = 150	initial time (s)	duration (s)	final time (s)
MN-nAR	150.00961	0.00093	150.01053
nAR-LS(HD)	150.01053	0.00631	150.01684
LS(HD)-BR(HD)	150.01684	0.00841	150.02525
LS(HD)-LS(VD)	150.01684	0.04233	150.05917
LS(VD)-BR(VD)	150.05917	0.00841	150.06758
LS(HD)-nAR	150.01684	0.00651	150.02335
LS(VD)-pAR	150.05917	0.00641	150.06558
nAr-MN	150.12135	0.00109	150.12244
pAR-nAR	150.06558	0.05454	150.12012
Handover reg duration		0.11283	

Table 4.5: signaling packets duration 5th Handover, CBR

This is the return of MN to its Home Domain. The times are very similar to the inter-domain handover in the opposite direction, 113 ms to registration, 122 ms since the start of the node's movement and 140 ms to receive the first packet of data in the new location. The packets that travel between the two domains still spend more time than all of the others.

4.4.1.2 – TCP Handovers

Figure 4.7 represent the duration of signaling packets in seconds during the handover of CN from BS0 to BS1 at 50s and the table 4.6 shows the times of the same packets.

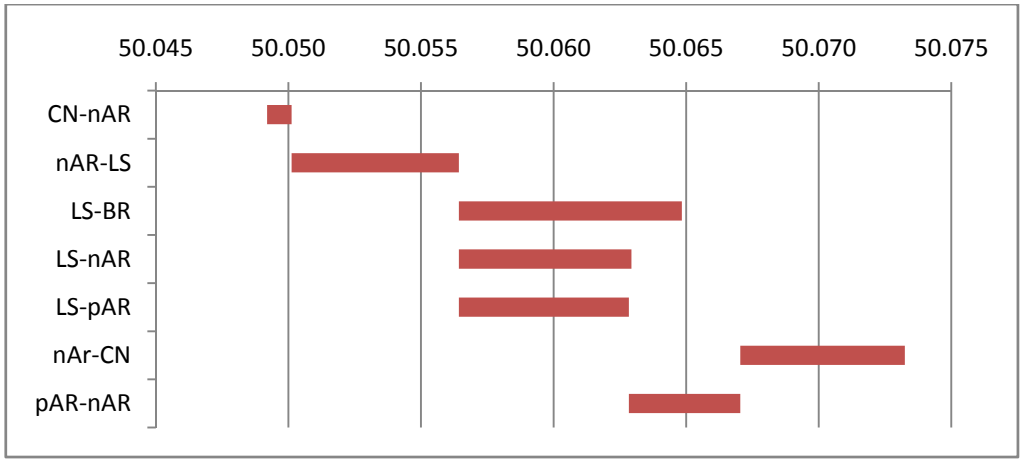

Figure 4.7: signaling packets duration 1st Handover, TCP

t0 = 50	initial time (s)	duration (s)	final time (s)
CN-nAR	50.04919	0.00093	50.05012
nAR-LS	50.05012	0.00631	50.05643
LS-BR	50.05643	0.00841	50.06484
LS-nAR	50.05643	0.00651	50.06294
LS-pAR	50.05643	0.00641	50.06284
nAr-CN	50.06704	0.00621	50.07325
pAR-nAR	50.06284	0.00420	50.06704
Handover reg duration		0.02406	

Table 4.6: signaling packets duration 1st Handover, TCP

Here the CN makes an intra-domain handover that had a registration duration of 24 ms and the total time spent was 73 ms. It's important to note that, as TCP uses the best rate possible and is a two way traffic protocol, since the sender also receives acknowledge packets, the network had more traffic so the CN-nAR message was only sent after almost 50ms of the movement start.

Figure 4.8 represent the duration of signaling packets in seconds during the handover of MN from BS2 to BS3 at 75s and the table 4.7 shows the times of the same packets.

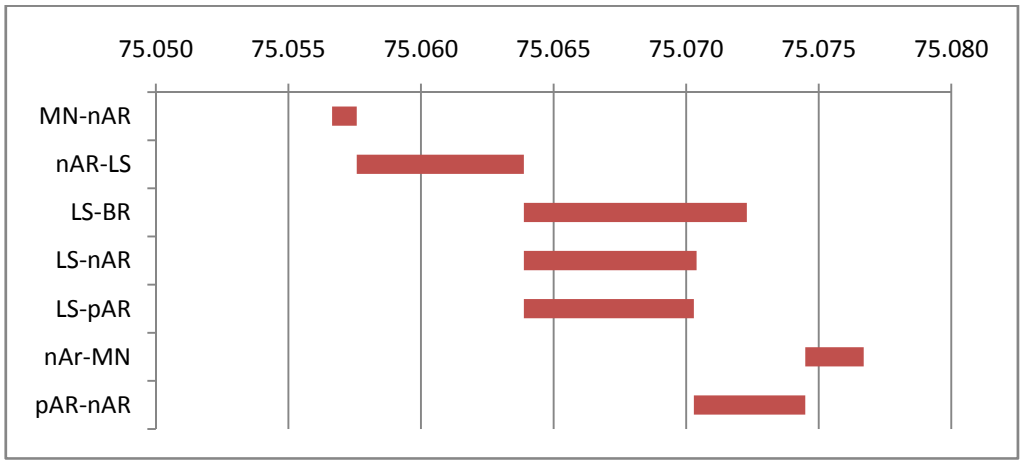

Figure 4.8: signaling packets duration 2nd Handover, TCP

t0 = 75	initial time (s)	duration (s)	final time (s)
MN-nAR	75.05665	0.00093	75.05757
nAR-LS	75.05758	0.00631	75.06388
LS-BR	75.06388	0.00841	75.07229
LS-nAR	75.06388	0.00651	75.07039
LS-pAR	75.06388	0.00641	75.07029
nAr-MN	75.07450	0.00220	75.07670
pAR-nAR	75.07029	0.00420	75.07450
Handover reg duration		0.02005	

Table 4.7: signaling packets duration 2nd Handover, TCP

In the intra-domain handover of MN, we found the same characteristics that in CN handover, the same small duration, 20 ms and the delay time to MN-nAR be sent that causes the total time of registration to be 77 ms. The first packet received in the MN was at 75.092 s.

Figure 4.9 represent the duration of signaling packets in seconds during the handover of MN from BS3 to BS0 at 100s and the table 4.8 shows the times of the same packets

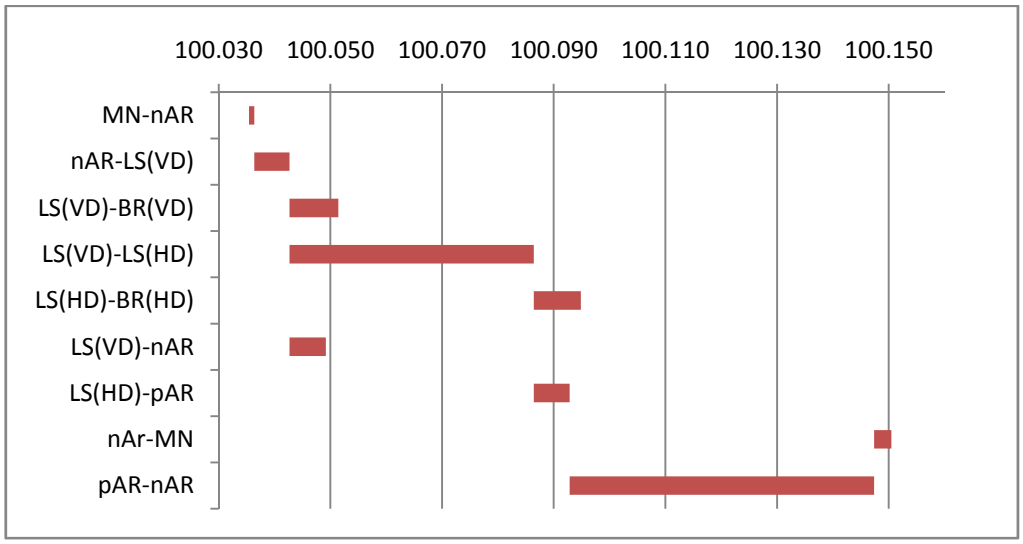

Figure 4.9: signaling packets duration 3rd Handover, TCP

t0 = 100	initial time (s)	duration (s)	final time (s)
MN-nAR	100.03543	0.00093	100.03636
nAR-LS(VD)	100.03636	0.00631	100.04267
LS(VD)-BR(VD)	100.04267	0.00876	100.05143
LS(VD)-LS(HD)	100.04267	0.04377	100.08643
LS(HD)-BR(HD)	100.08643	0.00841	100.09484
LS(VD)-nAR	100.04267	0.00651	100.04918
LS(HD)-pAR	100.08643	0.00641	100.09284
nAr-MN	100.14738	0.00311	100.15049
pAR-nAR	100.09284	0.05454	100.14738
Handover reg duration		0.11506	

Table 4.8: signaling packets duration 3rd Handover, TCP

In the inter-domain handover from Home Domain to Visited Domain the duration is 115ms, approaching to the duration using CBR and two inter-domain messages filling most of the registration time, the same delay in the beginning as occurs in the other handover with TCP, a total duration time of 150ms and a first packet received in MN at 150.163s.

Figure 4.10 represent the duration of signaling packets in seconds during the handover of MN from BS0 to BS1 at 125s and the table 4.9 shows the times of the same packets.

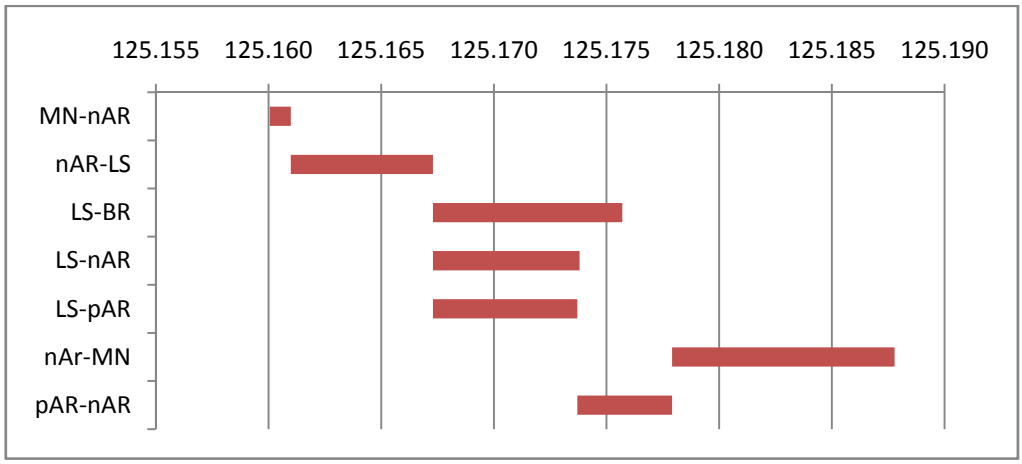

Figure 4.10: signaling packets duration 4th Handover, TCP

t0 = 125	initial time (s)	duration (s)	final time (s)
MN-nAR	125.16006	0.00093	125.16099
nAR-LS	125.16099	0.00631	125.16729
LS-BR	125.16729	0.00841	125.17570
LS-nAR	125.16729	0.00651	125.17381
LS-pAR	125.16729	0.00641	125.17370
nAr-MN	125.17791	0.00988	125.18778
pAR-nAR	125.17370	0.00420	125.17791
Handover reg duration		0.02773	

Table 4.9: signaling packets duration 4th Handover, TCP

In this handover it's needed pay attention to the fact that the two nodes, CN and MN are served by the same BS, both send and receive packets and TCP force the maximum rate that it can get. So it was as 160 ms delay to send the first registration packet. After that everything occurred normally with a 28ms registration time and a data packet arriving 30ms after the registration was over.

Figure 4.11 represent the duration of signaling packets in seconds during the handover of MN from BS1 to BS2 at 150s and the table 4.10 shows the times of the same packets.

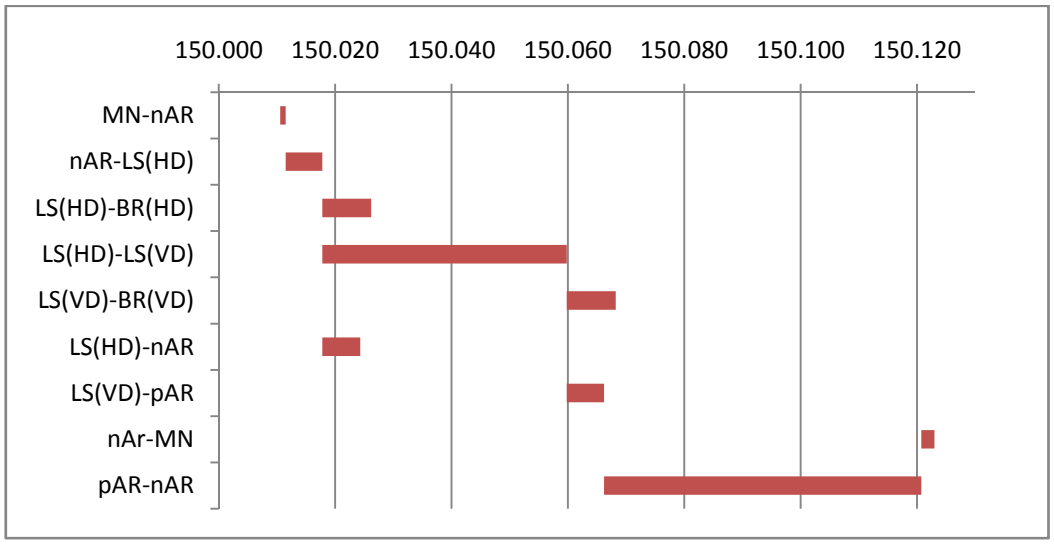

Figure 4.11: signaling packets duration 5th Handover, TCP

t0 = 150	initial time (s)	duration (s)	final time (s)
MN-nAR	150.01056	0.00093	150.01149
nAR-LS(HD)	150.01149	0.00631	150.01780
LS(HD)-BR(HD)	150.01780	0.00841	150.02621
LS(HD)-LS(VD)	150.01780	0.04202	150.05982
LS(VD)-BR(VD)	150.05982	0.00841	150.06823
LS(HD)-nAR	150.01780	0.00651	150.02431
LS(VD)-pAR	150.05982	0.00641	150.06623
nAr-MN	150.12077	0.00224	150.12301
pAR-nAR	150.06623	0.05454	150.12077
Handover reg duration		0.11244	

Table 4.10: signaling packets duration 5th Handover, TCP

In the return to the Home Domain it's visible that the delay is smaller since this domain hasn't traffic until MN returns and the times are similar to the other simulations, 112 ms to registration, 123ms from the beginning of the movement at 150 ms until the last registration message was received and the first data packet was received at 150.187s.

In general the handover registration duration, using CBR traffic, have sensibly the same duration, no matter where the mobile node moves and which domain it belongs. The same occurs with inter-domain handover despite the time of registrations was higher than in intra-domain.

Inter-domain registration's handovers are very dependent from the distance between the two domains and when it is bigger the problems can be it too.

Using TCP, the registration suffered some delays because this kind of protocol uses the network with the best rate it can and have acknowledge packets that travels in the opposite direction to detect and avoid packet loss. With these two mechanisms the network has more delays and if the ESM registration packets aren't priority in wireless links, as in this scenario, the time between the movement of mobile node and the sending of the router solicitation could be significant. The justification to the rtSol message not being defined as priority in simulations is that, despite being represented and treated as a registration message, in NS-2, it is an independent message between MNs and AR, generated by Neighbor Discovery and not a part of the ESM architecture, where the registration is done only by the network without MN intervention.

In the simulation, between the time 125s and 150s, the two mobile nodes are served by the same BS which causes a reduction of the bandwidth of each one and more difficult in the registration on the handover at 125s.

4.4.2 - Throughput

Throughput results were tested only in TCP, since CBR has a constant bit rate. This was measured in intervals of 2ms.

One entire simulation with all five handovers.

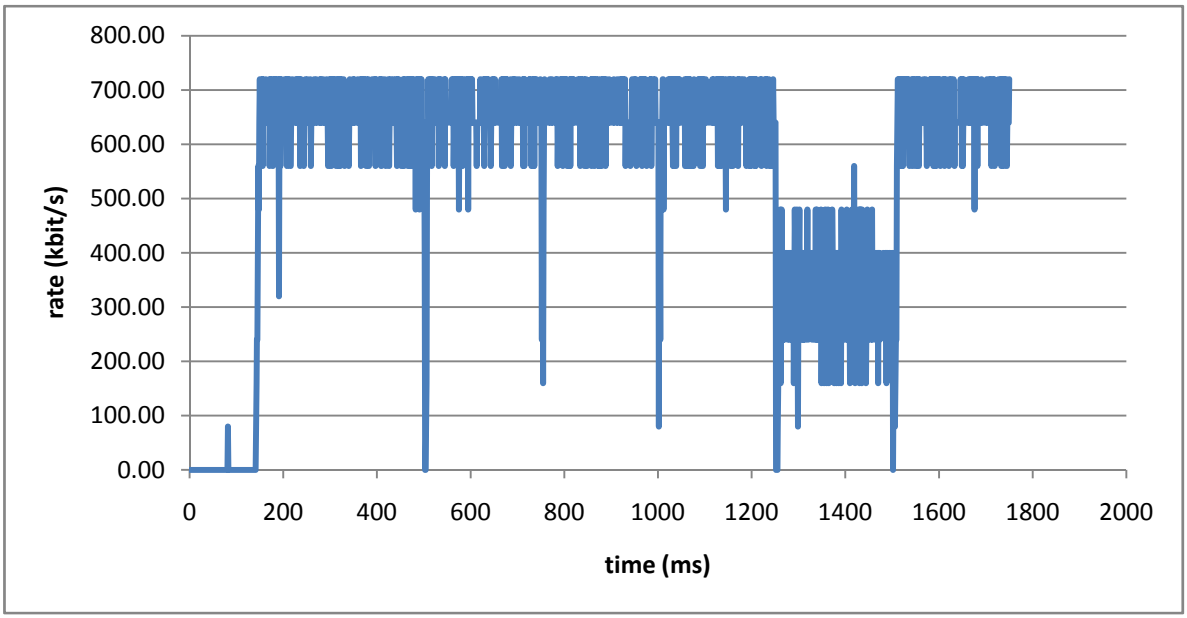

Figure 4.12: throughput of one entire simulation

Figure 4.12 shows the throughput, in the total time of a simulation, it is easy to note a mean of 640 kbps, except between 125s and 150s; that is 320kbit/s because CN and MN are served by the same BS and so the rate is half of the rate in the rest of simulation. The traffic was started at 14s and it's possible to see the handovers that occurred when the rate has a negative peak almost near zero, at the times of: 50s, 75s, 100s, 125s and 150s.

Handover of CN from BS0 to BS1 at 50s

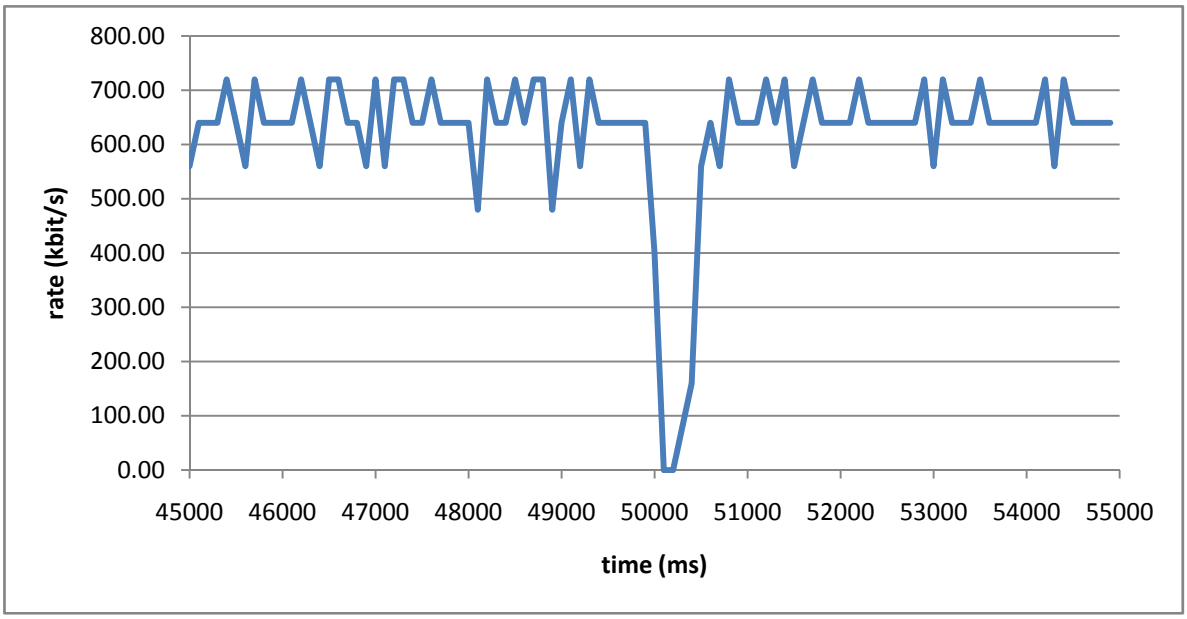

Figure 4.13: throughput of 1st Handover

Handover of MN from BS2 to BS3 at 75s

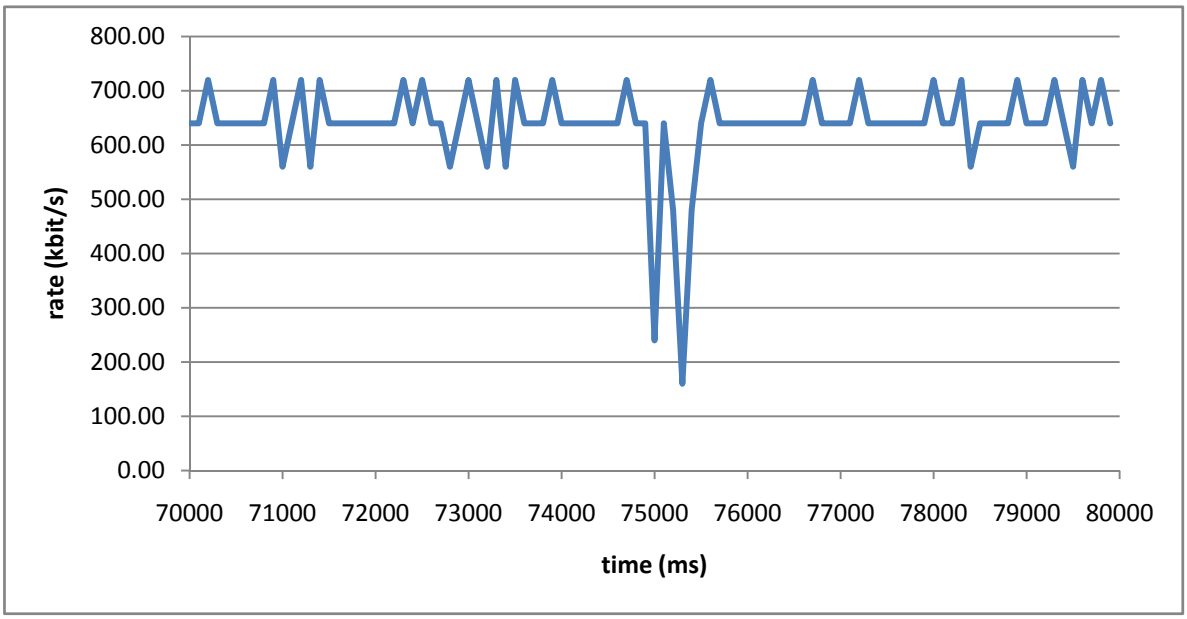

Figure 4.14: throughput of 2nd Handover

Handover of MN from BS3 to BS0 at 100s

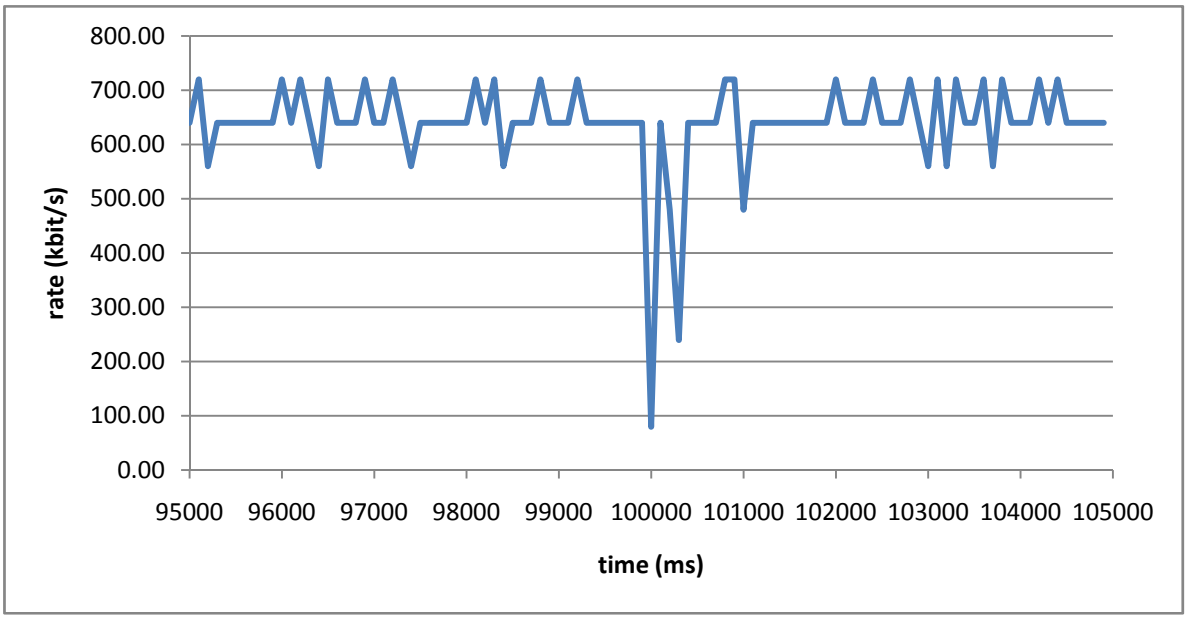

Figure 4.15: throughput of 3rd Handover

Handover of MN from BS0 to BS1 at 125s

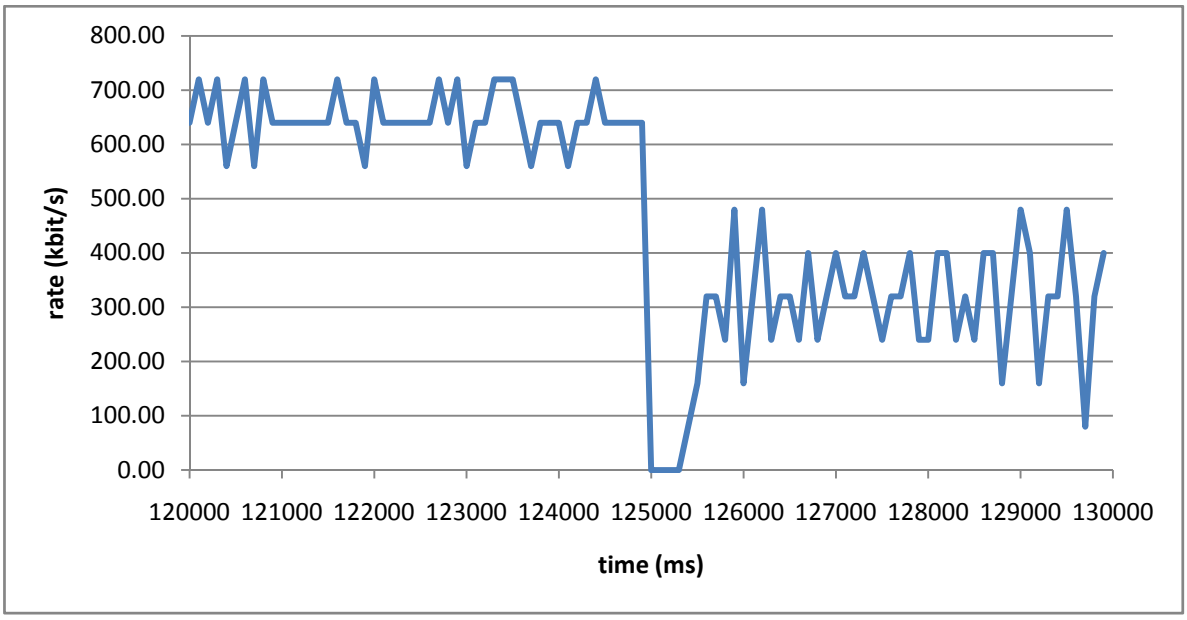

Figure 4.16: throughput of 4th Handover

Handover of MN from BS1 to BS2 at 150s

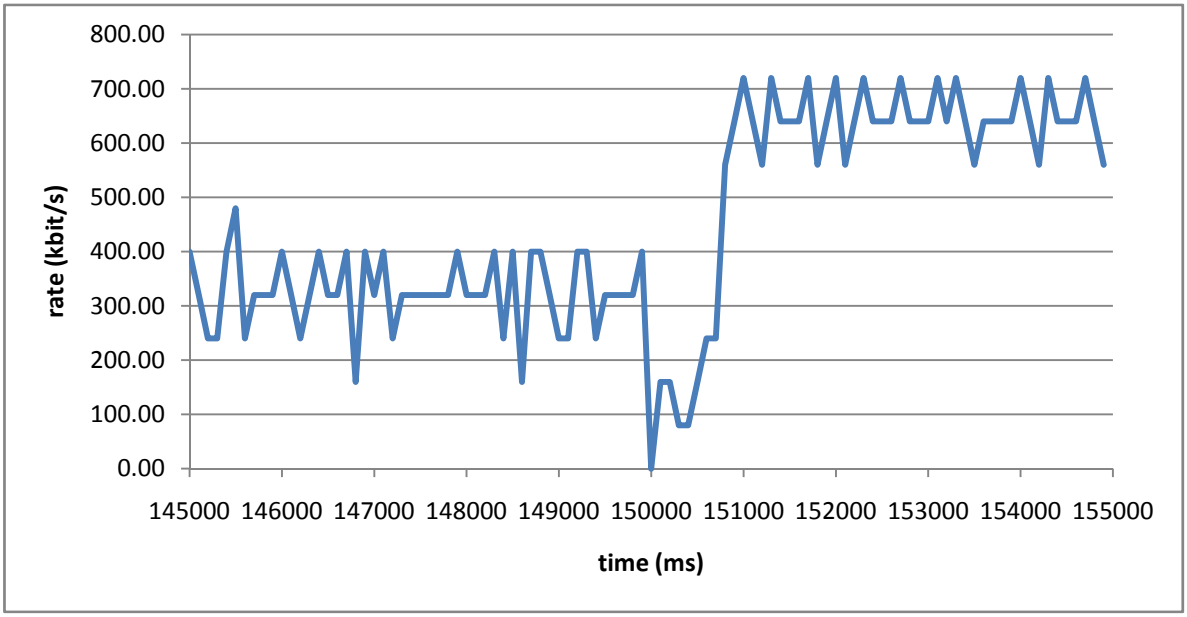

Figure 4.17: throughput of 5th Handover

Figures 4.13 to 4.17 represent a close up of each handover tested in simulation. The time of the negatives peaks is almost the same in the different handovers, it takes near 500ms to stabilize the throughput, not including the handovers of time 125s and 150s because the throughput mean suffers biggest differences before and after handovers.

4.4.3 - Loss

Loss of packets in the total time of simulation was tested only for CBR traffic, since TCP has a loss protection mechanism. The simulation had the usual five diferent handovers.

interval per pkt (ms)	rate (Kb/s)	no. Packets loss						
		total	HO50	HO75	HO100	HO125	HO150	total HOs
160.000	50	2	0	0	0	2	0	2
80.000	100	1	0	1	0	0	0	1
53.333	150	3	0	0	1	2	0	3
40.000	200	2	0	0	1	1	0	2
32.000	250	5	1	1	1	1	1	5
26.667	300	7	2	1	2	1	1	7
22.857	350	8	2	1	1	2	2	8
20.000	400	5	0	2	2	1	0	5
18.824	425	28	1	2	1	3	2	9
17.778	450	138	3	1	1	4	7	16
16.842	475	241	1	2	1	8	4	16
16.000	500	345	3	2	2	3	4	14
15.238	525	411	5	2	2	9	3	21
14.545	550	481	0	1	3	5	3	12
13.913	575	520	3	2	4	3	2	14
13.333	600	641	0	3	4	6	2	15
12.800	625	739	5	3	4	4	8	24
12.308	650	801	5	3	4	8	3	23
11.852	675	845	5	2	4	4	5	20
11.429	700	1012	5	3	4	8	7	27

Table 4.11: lost packets

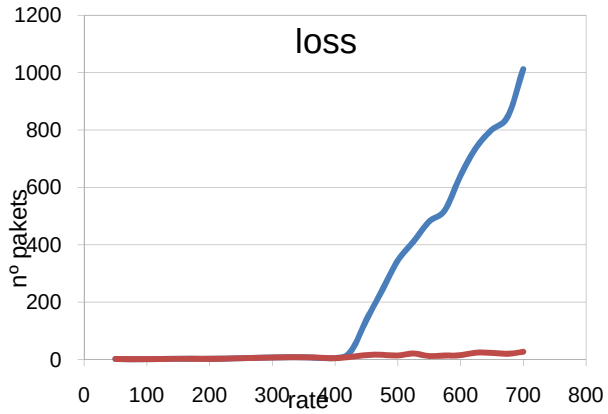

Figure 4.18: packet loss (legend: blue - total pkt; red - HO pkt)

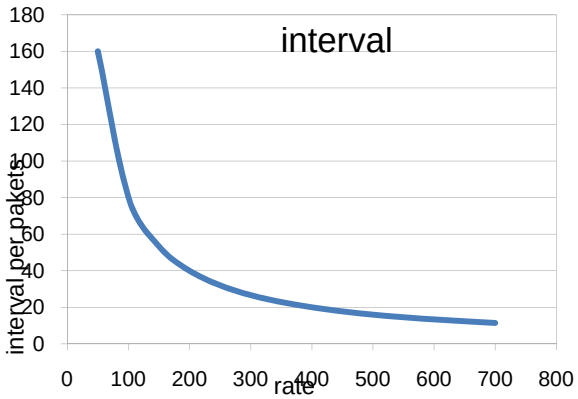

Figure 4.19: interval per packets

In the Table 4.11 and the Figure 4.18 (in blue) it's possible to see that the total lost packets increase very much when CBR increases beyond the rate of 450 kbps. After that the network starts to saturate and the queues start to be full because the total bandwidth is only 5Mb. However the loss packets during the handovers (in red on Figure 4.18) are very small comparing to the total, so almost lost packets were caused by network saturation and not for the time that the registration takes in each handover.

4.4.4 – Load in LSs

Handover intra-domains using CBR at 75s

	time			
delay (ms)	tp mov (s)	tp finish reg (s)	tp 1st pkt recv (s)	duration
2	75	75.03011	75.04374	0.03011
10	75	75.04503	75.07469	0.04503
20	75	75.06549	75.10616	0.06549
30	75	75.08603	75.10632	0.08603
40	75	75.10523	75.13699	0.10523
50	75	75.12583	75.13699	0.12583
60	75	75.14002	75.17511	0.14002
70	75	75.16531	75.19965	0.16531
80	75	75.17958	75.19374	0.17958
90	75	75.20032	75.22511	0.20032
100	75	75.21998	75.25630	0.21998
110	75	75.23994	75.25616	0.23994
120	75	75.26000	75.28735	0.26000
130	75	75.27982	75.29969	0.27982
140	75	75.30553	75.32519	0.30553
150	75	75.32579	75.35654	0.32579
160	75	75.34607	75.35627	0.34607
170	75	75.36581	75.38747	0.36581
180	75	75.38581	75.41836	0.38581
190	75	75.40641	75.41844	0.40641
200	75	75.41974	75.45618	0.41974
210	75	75.44575	75.48120	0.44575
220	75	75.46008	75.49138	0.46008
230	75	75.48034	75.49176	0.48034
240	75	75.49982	75.52207	0.49982
250	75	75.51962	75.55584	0.51962

Table 4.12: Handover duration with load in LS, CBR, intra-domain

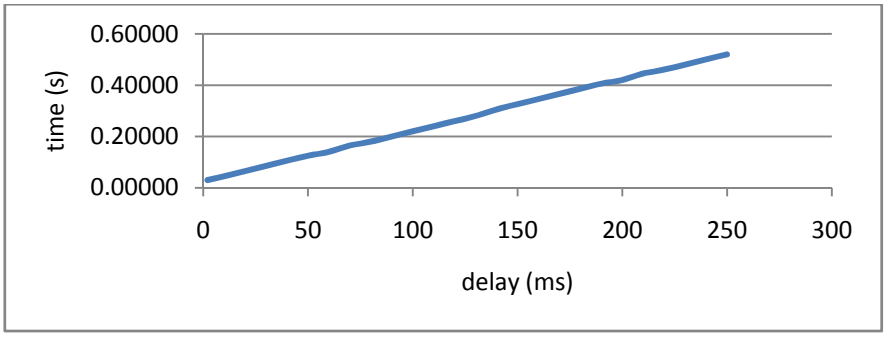

Figure 4.20: Handover duration with load in LS, CBR, intra-domain

Handover inter-domains using CBR at 100s

	time			
delay (ms)	tp mov (s)	tp finish reg (s)	tp 1st pkt recv (s)	duration
2	100	100.11348	100.12559	0.11348
10	100	100.17754	100.18777	0.17754
20	100	100.25797	100.28198	0.25797
30	100	100.34647	100.37549	0.34647
40	100	100.41992	100.43815	0.41992
50	100	100.50302	100.53208	0.50302
60	100	100.57756	100.60047	0.57756
70	100	100.65887	100.68783	0.65887
80	100	100.74623	100.77543	0.74623
90	100	100.82777	100.83797	0.82777
100	100	100.90825	100.93162	0.90825
110	100	100.98461	100.99480	0.98461
120	100	101.06433	101.08821	1.06433
130	100	101.13784	101.16289	1.13784
140	100	101.22185	101.25077	1.22185
150	100	101.29754	101.31337	1.29754
160	100	101.37922	101.40662	1.37922
170	100	101.47183	101.50057	1.47183
180	100	101.53776	101.56291	1.53776
190	100	101.62780	101.65722	1.62780
200	100	101.69707	101.72581	1.69707
210	100	101.78393	101.81291	1.78393
220	100	101.85790	101.88559	1.85790
230	100	101.93730	101.94837	1.93730
240	100	102.01734	102.04214	2.01734
250	100	102.09720	102.10707	2.09720

Table 4.13: Handover duration with load in LS, CBR, inter-domain

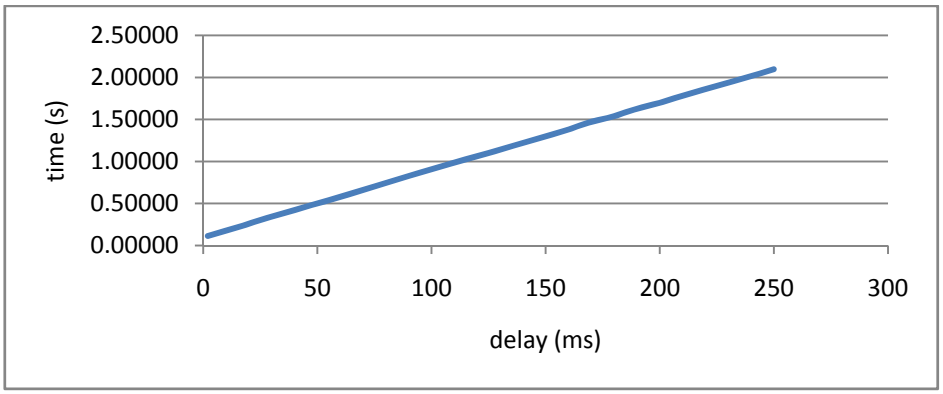

Figure 4.21: Handover duration with load in LS, CBR, inter-domain

Handover intra-domains using TCP at 75s

	time			
delay (ms)	tp mov (s)	tp finish reg (s)	tp 1st pkt recv (s)	duration
2	75	75.05681	75.07673	0.05681
10	75	75.10038	75.11349	0.10038
20	75	75.09341	75.13235	0.09341
30	75	75.13135	75.14814	0.13135
40	75	75.13398	75.18871	0.13398
50	75	75.16008	75.32202	0.16008
60	75	75.18975	75.24694	0.18975
70	75	75.17290	75.18889	0.17290
80	75	75.19292	75.21176	0.19292
90	75	75.21312	75.23236	0.21312
100	75	75.23330	75.64150	0.23330
110	75	75.27978	75.32792	0.27978
120	75	75.30042	75.32846	0.30042
130	75	75.31165	75.35793	0.31165
140	75	75.34475	75.36450	0.34475
150	75	75.36489	75.38399	0.36489
160	75	75.38956	75.38956	0.38956
170	75	75.39123	75.40825	0.39123
180	75	75.41159	76.00752	0.41159
190	75	75.43183	76.00756	0.43183
200	75	75.46551	75.77422	0.46551
210	75	75.48581	75.77422	0.48581
220	75	75.50913	75.52113	0.50913
230	75	75.52925	76.25910	0.52925
240	75	75.54887	76.25910	0.54887
250	75	75.56949	76.25910	0.56949

Table 4.14: Handover duration with load in LS, TCP, intra-domain

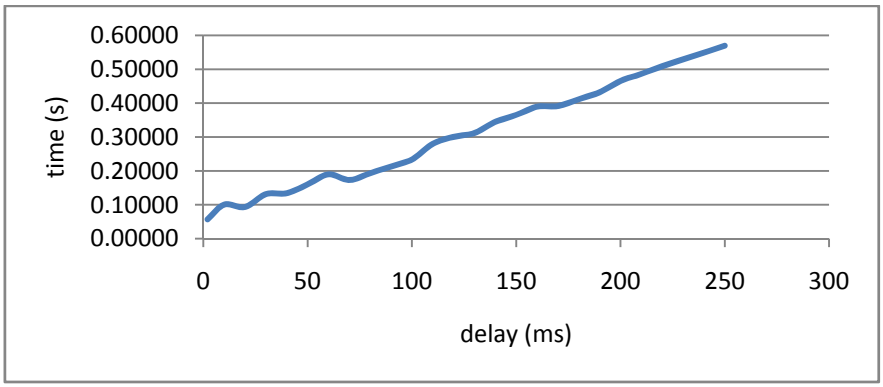

Figure 4.22: Handover duration with load in LS, TCP, intra-domain

Handover inter-domains using TCP at 100s

	time			
delay (ms)	tp mov (s)	tp finish reg (s)	tp 1st pkt recv (s)	duration
2	100	100.15944	100.16954	0.15944
10	100	100.22648	100.34822	0.22648
20	100	100.26836	100.37931	0.26836
30	100	100.37705	100.38699	0.37705
40	100	100.45995	100.55912	0.45995
50	100	100.54409	100.55855	0.54409
60	100	100.62668	100.63704	0.62668
70	100	100.70495	100.71527	0.70495
80	100	100.77238	100.80971	0.77238
90	100	100.82539	100.83752	0.82539
100	100	100.91078	100.92291	0.91078
110	100	101.02943	101.04403	1.02943
120	100	101.10415	101.11854	1.10415
130	100	101.15478	101.16505	1.15478
140	100	101.26388	101.27809	1.26388
150	100	101.31864	101.32883	1.31864
160	100	101.43280	101.44498	1.43280
170	100	101.50901	101.51905	1.50901
180	100	101.59733	101.60980	1.59733
190	100	101.68112	101.69114	1.68112
200	100	101.75221	101.76960	1.75221
210	100	101.83988	101.85219	1.83988
220	100	101.89020	101.90255	1.89020
230	100	101.94792	101.96461	1.94792
240	100	102.02616	102.03655	2.02616
250	100	102.11153	102.12207	2.11153

Table 4.15: Handover duration with load in LS, TCP, inter-domain

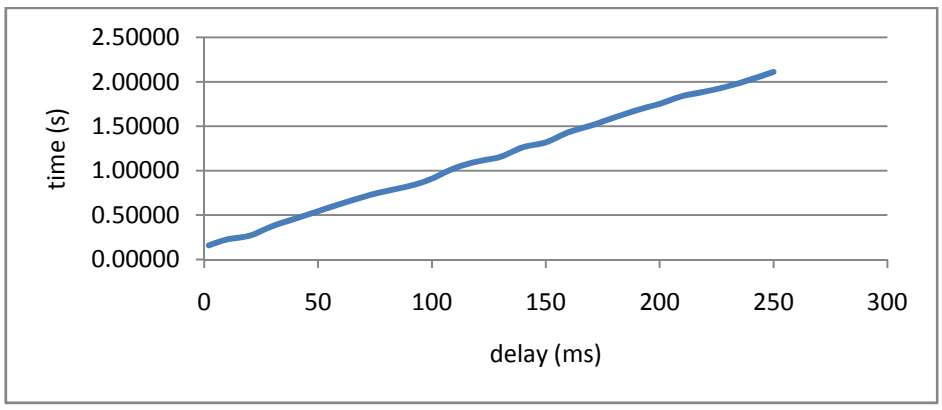

Figure 4.23: Handover duration with load in LS, TCP, inter-domain

With the increase of the delay in links that connect to LSs, it we want to study the effect of the load in the location service like what happens when there are many mobile nodes and LS needs to control all positions. So the simulations comprehend CBR and TCP traffic in all five handovers, but since the results were very similar, we only show an intra-domain and one inter-domain handover of each kind of traffic.

The result (shown in Figures 4.20 to 4.23 and tables 4.12 to 4.15) is that when increases in the load in the LSs also increases the time that registration takes, with arithmetic proportions and this is valid to all kind of traffic and all kind of handovers. The difference that in CBR the graphic is more stable than in TCP is because CBR has a constant rate and TCP don't. The inter-domain handover suffers more with the increase of the load because they need two LS in each registry.

4.4.5 – Load on inter-domain link

Handover inter-domains using CBR at 100s

	time			
delay (ms)	tp mov (s)	tp finish reg (s)	tp 1st pkt recv (s)	duration
2	100	100.06724	100.07981	0.06724
25	100	100.11340	100.12573	0.11340
50	100	100.16352	100.18563	0.16352
75	100	100.21160	100.22363	0.21160
100	100	100.26364	100.27513	0.26364
125	100	100.31320	100.33160	0.31320
150	100	100.36342	100.38178	0.36342
175	100	100.42772	100.45686	0.42772
200	100	100.46360	100.47555	0.46360
225	100	100.51338	100.52577	0.51338
250	100	100.56296	100.57565	0.56296
275	100	100.61316	100.62523	0.61316
300	100	100.67824	100.70726	0.67824
325	100	100.71390	100.72561	0.71390
350	100	100.76522	100.79484	0.76522

Table 4.16: Handover duration with load in inter-domain link, CBR

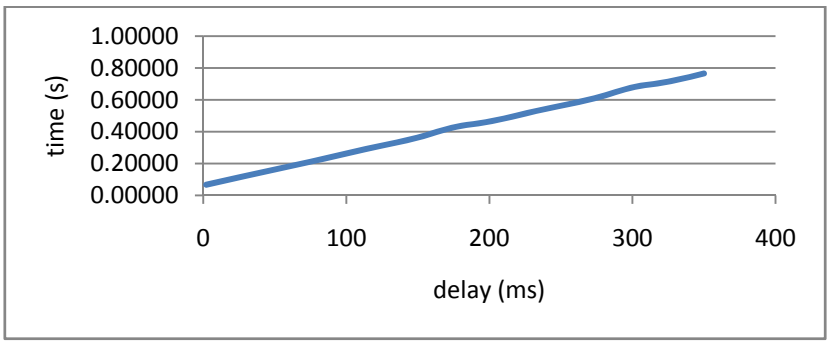

Figure 4.24: Handover duration with load in inter-domain link, CBR

Handover inter-domains using TCP at 100s

	time			
delay (ms)	tp mov (s)	tp finish reg (s)	tp 1st pkt recv (s)	duration
2	100	100.10351	100.11795	0.10351
25	100	100.15944	100.16954	0.15944
50	100	100.17235	100.18446	0.17235
75	100	100.26388	100.27817	0.26388
100	100	100.27459	100.28683	0.27459
125	100	100.32284	100.33332	0.32284
150	100	100.37103	100.40128	0.37103
175	100	100.42795	100.43800	0.42795
200	100	100.46791	100.48265	0.46791
225	100	100.51294	100.52563	0.51294
250	100	100.57086	100.58796	0.57086
275	100	100.63297	100.64349	0.63297
300	100	100.66376	100.85199	0.66376
325	100	100.71645	100.72959	0.71645
350	100	100.76736	100.76868	0.76736

Table 4.17: Handover duration with load in link inter-domain, TCP

Handover duration

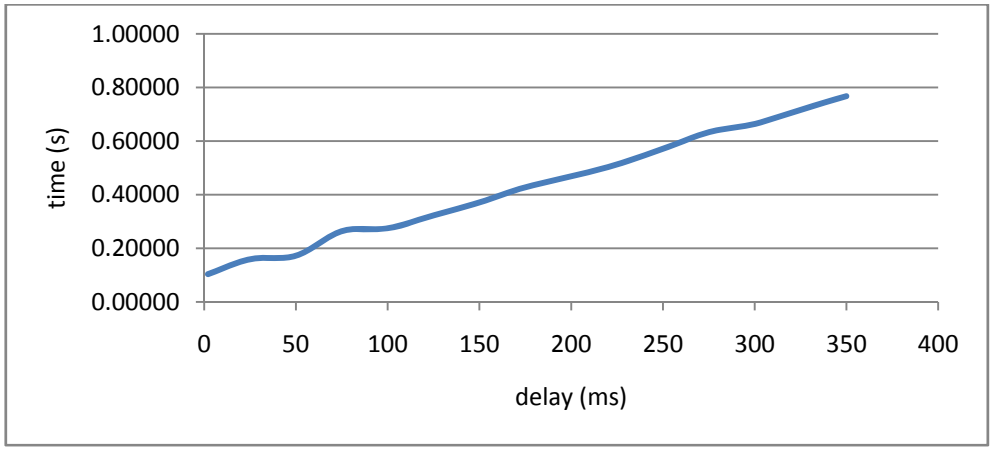

Figure 4.25: Handover duration with load in inter-domain link, TCP

To study the effects of the distance between the two domains and the load between them the delay in the inter-domain link was increased in the simulated topology. This time it only makes sense to study the behavior in the inter-domain handovers but

once more the results were very similar, so it will only be presented one handover by traffic type.

The results (represented in Figures 4.24and 4.25; tables 4.16 and 4.17) show that the more load the inter-domain link has, the more time was needed to registration to be succeeded. The graphic shows a line with arithmetic proportions and without great variations in the two kinds of traffic, but this line increases slower than when was tested the load on LSs.

Chapter 5

Conclusions

During this work we have study IP mobility with some intra and inter-domain mechanism focus in one, Eppur si muove. The main objective was testing ESM behavior. To do this we discuss some aspects of this mechanism, especially in intra-domain mobility, were we made some extensions to the initial proposal. Then it was simulated using NS-2, tested and the results were analyzed.

After this work the greatest conclusion to take is that, in IP mobility, the big problems appear to remain in inter-domain mobility.

ESM proves to be efficient and fast solution with small handover times and good responses to load tests. Despite the intra-domain behavior, it deserves a good grade in intra-domain mobility. When it operates inter-domain, it starts to be slower and a less successful mechanism. As it was shown in Chapter 4 the mean of intra-domain handover registration is 22ms and for inter-domain is 112ms, so inter-domain has a duration 5 times superior than intra-domain. In the loss test, the inter-domain handovers had little more loss packets than intra-domain, but both had very few packets lost. On the load tests the effects were felt more on the inter-domain handover too, but the network had the normal behavior to those conditions. On the throughput the time to stabilize was too short and didn't affect TCP behavior.

The fact that the domains need to interact between them and have separate administrations is one of the biggest problems. All works well if different domains can act like if they are only one, if the trust between them is 100% which means all free administrative traffic and information exchange. But since most of them belong to concurrent companies this will only exist in an utopist future, so it is needed to improve

the federations' solution turning it in an interesting solution to ISPs and other operators of the IP's networks.

The differences from inter-domain to intra-domain behavior are not exclusive from ESM and it can be extended to all architectures that work in this field. There is still a lot of work to do in this area. In ESM, for example, it is still missing a mechanism that detects when a mobile node turns off, that alerts the LS of the last domain where it was connected to update the information on the rest of the network and to save the last known location. Thus is needed to find a way to work with flat IP networks using the networks that we have nowadays allowing the free movement of nodes without changing IP addresses.

However this is the beautiful of life: using the present to prepare the future.

Bibliography

[1] Debalina Ghosh, *"Mobile IP"*, in http://www.acm.org/crossroads/xrds7-2/mobileip.html

[2] R. Koodli, *"Fast Handovers for Mobile IPv6"* in *RFC 4068*, IETF, July 2005

[3] H. J. Lee, S. J. Lee, J. H. Yoon, D. H. Cheon and J. I. Lee, **"**Mobile IPv6 Fast Handovers for 802.11 Networks" in *RFC 4269*, IETF, November 2005

[4] J. Xie, I. Howitt, and I. Shibeika, **"**IEEE 802.11-based Mobile IP Fast Handoff Latency Analysis" in *IEEE International Conference on Communications*, IEEE, 2007

[5] S. Menezes, S.Venkatesan and K. H. Rho, "An Efficient Handover Scheme Based on Fast Mobile IPv6" in *Vehicular Technology Conference*, IEEE, 2006

[6] Z. Zhang, J. Fang, W. Wang and S. Zhang, "*Performance Comparison of Mobile IPv6 and Its Extensions"* in *Wireless Communications, Networking and Mobile Computing, 2007. (WiCom 2007). International Conference on*, IEEE, 2007

[7] X. Perez-Costa, M. Torrent-Moreno and H. Hartenstein, *"A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination" in Mobile Computing and Communications Review*, Volume 7, Number 4, ACM, 2003

[8] L. Osborne, A. Abdel-Hamid and R. Ramadugu, "A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6 and Mobile IPv6 Regional Registrations", *in International Conference on Wireless Networks, Communications and Mobile Computing*, IEEE, 2005

[9] P. Estrela**, "**Protocolos de Mobilidade para Terminais IP" in *Master thesis on Engenharia Informática e de Computadores*, IST, January, 2003

[10] I. Vicente H. and E. Quiroz M., "Performance analysis of the Cellular IP mobility protocol", in *Proceedings of the Electronics, Robotics and Automotive Mechanics Conference (CERMA'06)*, IEEE, 2006

[11] A. Campbell, J. Gomez, S. Kim, A. Valkó, "Design, Implementation, and Evaluation of Cellular IP" in *Personal Communications*, IEEE, August 2000

[12] R. Ramjee*,* K. Varadhan, L. Salgarelli, S. R. Thuel, S. Wang, and T. La Porta, "HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks*"* in *IEEE/ACM Transactions on networking, vol. 10, no. 3*, IEEE, June 2002

[13] I. Guardini, G. Giaretta and F. Miconi “Performance analysis of a network-based protocol for localized IP mobility management” in *Communications, 2007. (ICC '07). IEEE International Conference on*, IEEE, 2007

[14] J. Laganier, M. Flege, A. Zugenmaier, A. Prasad and J. Kempf, J. Wood, “Travelling without Moving: 802.11 Access Points backed by Secure NETLMM” in *Computer Communications and Networks, 2007. (ICCCN 2007). Proceedings of 16th International Conference on*, IEEE, 2007

[15] J. S. Khoury, H. N. Jerezt and C. T. Abdallah “Efficient User Controlled Inter-Domain SIP Mobility Authentication, Registration, and Call Routing” in *Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007). Fourth Annual International Conference on*, IEEE, 2007

[16] J. S. Khoury, H. N. Jerezt and C. T. Abdallah *“H-SIP Inter-Domain SIP Mobility: Desig*n” in *Consumer Communications and Networking Conference, 2007. (CCNC 2007). 4th IEEE*, IEEE, 2007

[17] E. Wedlund and H. Schulzrinne “Mobility Support using SIP” in *International Workshop on Wireless Mobile Multimedia*, ACM, 1999

[18] V. Jesus, H. Santos, A. Matos, S. Sargento and R. L. Aguiar, “A Terminal Mobility Architecture” (work in Progress), 2007

[19] V. Jesus, “The Daidalos Federation Architecture” in *ICT Mobile Summit 2008*, 2008

[20] A. Diab, A. Mitschele-Thiel and R. Boeringer, “A Framework to Support Fast Inter-domains Mobility in All-IP” in 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06), IEEE, 2006

[21] T. Takahashi, J. Harju, K. Asatani, H. Tominaga, “Inter-domain Handover Scheme based on Forwarding Router Discovery for Mobile IP Networks” in *Wireless Communications and Networking Conference, 2005 (WCNC 2005)*, IEEE, 2005

[22] C. de Laat, G. Gross, L Gommans, J. Vollbrecht and D. Spenc, “Generic AAA Architecture”, in *RFC 2903*, IETF, August 2000